University of Chicago Legal Forum

Volume 2008 | Issue 1 Article 2

Good enough Privacy

Paul Ohm
Paul.Ohm@chicagounbound.edu

Articles

Good Enough Privacy†

Paul Ohm‡

INTRODUCTION

A decade ago, the National Security Agency ("NSA") declassified two encryption protocols called Skipjack and KEA.[1] There was no official ceremony; the event was hardly marked by the media.[2] The protocols quietly slipped out of their secret walled garden into the unclassified world of public knowledge. It was a whispered denouement closing one of the most cacophonous, roiling public arguments in the history of technological privacy—the Clipper Chip debate.

---

‡ Associate Professor, University of Colorado Law School. Thanks to the editors of the *University of Chicago Legal Forum* for inviting me to present and publish this work and to the attendees of the "Law in a Networked World" symposium for their excellent comments and questions. Thanks also to Brad Bernthal, Nestor Davidson, Pierre de Vries, Ed Felten, Scott Moss, and Phil Weiser for their valuable contributions.

[1] *US DoD to Declassify Skipjack and Kea*, Telecomworldwire (June 25, 1998), available at <http://findarticles.com/p/articles/mi_m0ECZ/is_1998_June_25/ai_50104311> (last visited Apr 3, 2008). KEA stands for the "Key Exchange Algorithm." National Institute of Standards and Technology, *Key Escrow System Glossary*, Document number KES-NIST-SYS-GLSY-U-R1 (Oct 1995), available at <http://csrc.nist.gov/tacdfipsfkmi/KeyEscrow SystemGlossary.txt> (last visited Apr 3, 2008).

[2] The reporting was limited to scientific publications and the trade press. See, for example, *Spooks Show Their Hand*, 159 New Scientist 2323 (Jul 4, 1998); *NSA Opens Door for Commercial Fortezza Card Development*, 186 Aerospace Daily & Def Rep 61 (June 25, 1998).

The Clipper Chip—a blanket name describing a bundle of various technologies—was the United States' response to the fear that encryption was upsetting the balance between those who want to speak privately and those who want to listen in.[3] After a century of relying on wiretaps for gathering evidence of crime and developing intelligence about threats to national security, many government entities, and in particular the FBI and NSA, worried that these capabilities would be lost in a cloud of encryption.[4]

The Clipper Chip was touted by its proponents as a way to use markets rather than government mandates to deal with the threat of encryption.[5] Rather than ban the use of encryption or dissemination of encryption tools, the government would encourage people to encrypt voice phone calls using a new, robust form of easy-to-use encryption invented presumably by the NSA. The catch was that the encryption contained a backdoor, and encrypted messages could be unlocked using keys held by the government "in escrow."[6] According to the plans, nobody would be forced to use Clipper, at least not initially.[7] If people chose to use it, they would get strong privacy against most of the world in return for giving up effective privacy against the government.

This Article analyzes the tools that provide or strip privacy online. Restating it neutrally, it is about tools that provide one of two opposing values: privacy or transparency.

This Article also seeks to reawaken a slumbering debate. A decade ago, a fierce argument about Clipper raged. Books were written,[8] computer scientists and industry officials weighed in,[9]

---

[3] See Whitfield Diffie and Susan Landau, *Privacy on the Line* 231–33 (MIT 1998).

[4] See id.

[5] See A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U Pa L Rev 709, 742–43 (1995). Some saw it much less charitably. A. Michael Froomkin, *It Came from Planet Clipper: The Battle over Cryptographic Key "Escrow"*, 1996 U Chi Legal F 15, 67 ("Clipper sought to use government standard-setting and buying power to rig the market.").

[6] See Froomkin, 143 U Pa L Rev at 831 (1995) (cited in note 5). See generally Froomkin, 1996 U Chi Legal F 15 (cited in note 5).

[7] FBI Director Louis Freeh was quoted on more than one occasion keeping open the possibility of mandated key escrow in the future. See Froomkin, 1996 U Chi Legal F at 66 (cited in note 5) (quoting Director Freeh, "[i]f five years from now . . . what we are hearing is all encrypted material that the FBI is unable to decipher, then the policy of relying on voluntary compliance with (escrowed encryption) will have to change.").

[8] See, for example, David Brin, *The Transparent Society* (Addison-Wesley 1998).

[9] See Dorothy Denning, *To Tap or Not to Tap*, 36 Commun of the Assoc for Computing Machinery 24 (Mar 1993), plus follow up responses.

as did legal scholars.[10] Then, the government discovered the peril of a market-based solution: market rejection. Very few vendors marketed Clipper Chip-embedded phones, and those that did sold very few units.[11]

An interesting thing happened next: in a short period of time, a churning, intense public discussion about the technologies of privacy and transparency ended abruptly, petering away almost to nothing.[12] A quiet phase began, and we are still in it. Three leading online privacy groups maintain web pages about encryption, yet none have updated these pages since 2001.[13] Likewise, the Department of Justice has not modified its cryptography web page since 2000.[14] Why did the debate end so suddenly? Perhaps the Clipper Chip's rejection was seen as decisive, regarded by its opponents as unambiguous victory and by its proponents as complete defeat. Maybe government officials were simply cowed by the withering criticism and went away to lick their wounds.

But this is a truce not an armistice. The public debate and healthy sense of engagement has ended, but the participants continue to think and talk about privacy and transparency within their own private communities.

---

[10] See, for example, James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U Cin L Rev 177, 202–03 (1997); Froomkin, 1996 U Chi Legal F 15 (cited in note 5); Lawrence Lessig, *The Path of Cyberlaw*, 104 Yale L J 1743 (1995). The most influential law review discussion of the Clipper Chip was an article by Michael Froomkin. Froomkin, 143 U Pa L Rev 709 (cited in note 5).

[11] Diffie and Landau, *Privacy on the Line* at 215 (cited in note 3) (citing 17,000 sales of the AT&T TSD 3600 telephone—which used the Clipper Chip—including 9,000 sales to the FBI in an attempt to seed the market).

[12] The Clinton administration followed Clipper with a few brief proposals, two derisively dubbed Son of Clipper and Clipper III, but none of these were pursued for long. Froomkin, 1996 U Chi Legal F at 33–34 (cited in note 5) (describing "Son of Clipper"); id at 50 (describing "Clipper III").

[13] Electronic Frontier Foundation, *Encryption Archive* (last entry dated Jan 13, 2000), available at <http://w2.eff.org/Privacy/Crypto/> (last visited Apr 3, 2008); Center for Democracy and Technology, *Cryptography* (last article dated Oct 18, 2001), available at <http://www.cdt.org/crypto/> (last visited Apr 3, 2008); Electronic Privacy Information Center, *Cryptography Policy* (last article dated Oct 17, 2001), available at <http://epic.org/crypto/> (last visited Apr 3, 2008).

[14] United States Department of Justice, Computer Crime and Intellectual Property Section, *Encryption and Computer Crime* (page last updated May 8, 2000), available at <http://www.usdoj.gov/criminal/cybercrime/crypto.html> (last visited Apr 3, 2008). This is not to say, however, that DOJ is ignoring cryptography. In late 2007, reports surfaced that DOJ tried to convince a judge to compel a defendant to divulge encryption keys. The judge ruled against compulsion. See Adam Liptak, *If Your Hard Drive Could Testify . . .*, NY Times A12 (Jan 7, 2008); Declan McCullagh, *Judge: Man Can't be Forced to Divulge Encryption Passphrase*, CNET News.com (Dec 14, 2007), available at <http://www.news.com/8301-13578_3-9834495-38.html> (last visited Apr 3, 2008).

In the meantime, the decade since Clipper has seen the evolution and creation of technologies unlike anything available during the last round. In 1994, cryptography was difficult to use and used by few,[15] and the debate centered on possibilities and predictions. In contrast, today, cryptography is available in software that millions of users install and use.

Consider another quiet news event, this one about the evolution of technological privacy. On October 17, 2007, the online service Skype, a replacement for the telephone used to conduct voice conversations over the Internet ("VoIP"), reached an important milestone. On that day, ten million Skype users logged in simultaneously for the first time.[16] Most of these users were not activists, taking a stand for Internet privacy; most were simply searching for an alternative to expensive, inconvenient traditional phone service. Little did they realize that they were also serving as an important example of the hopes and fears of many who think about technological privacy.

By default, Skype surrounds every voice conversation in an unbreakable tunnel of encryption.[17] It is impossible to wiretap a Skype conversation, at least using traditional methods.[18] If Alice were to talk to Bob using Skype, then Eve, sitting on a wire somewhere between the pair, would be unable to decipher what they were saying.[19]

---

[15] See Alma Whitten and J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, Proceedings of the 8th USENIX Security Symposium 169–84 (Aug 23–26, 1999) available at <http://www.usenix.org/events/sec99/full_papers/whitten/whitten_html/> (last visited Apr 3, 2008) ("We conclude that PGP 5.0 is not usable enough to provide effective security for most computer users.").

[16] Villu Arak, *Stop and Hear the Sound of Skype Passing the 10 Million Simultaneous Users Mark*, Share Skype Blog (Oct 17, 2007), available at <http://share.skype.com/sites/en/2007/10/stop_and_hear_the_sound_of_sky.html> (last visited Apr 3, 2008).

[17] Tom Berson, Anagram Laboratories, *Skype Security Evaluation* ALR-2005-031 (Oct 18, 2005), available at <http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf> (last visited Apr 3, 2008) (white paper of consultant hired to assess Skype's encryption implementation); Jaanus Kase, *Skype Security and Encryption Review Now Available*, Share Skype Blog (Oct 21, 2005), available at <http://share.skype.com/sites/security/2005/10/skype_security_and_encryption.html> (last visited Apr 3, 2008).

[18] Peter Svensson, Associated Press, *Skype Use May Make Eavesdropping Passe*, USA Today.com (Feb 16, 2006), available at <http://www.usatoday.com/tech/news/computersecurity/2006-02-16-skype-wiretapping_x.htm> (last visited Apr 3, 2008) ("[A]ccording to [security expert Bruce Schneier], if Skype's encryption is weaker than believed, it still would stymie the kind of broad eavesdropping that the National Security Agency is reputed to be performing.").

[19] It is an age-old cryptographers' convention to populate encryption and wiretapping hypotheticals with speakers named Alice and Bob (and Carol and Ted); eavesdroppers/would-be decrypters are always named Eve. Diffie and Landau, *Privacy on the Line* at 18 (cited in note 3).

To some, Skype provides the technological privacy all users need and deserve.[20] Many who feel this way go beyond mere advocacy by programming, improving, distributing, or funding Skype or similar projects.[21] To others, the millions of Skype-encrypted tunnels tentacling throughout the Internet are a threat to security, a creeping web of technologically-created evasion and subterfuge, enabling and emboldening evil people to do evil things without fear of detection.[22]

Who has the better argument? Should Skype be banned or pre-installed on every new computer? If, instead of these alternatives, you want a third choice, something in between these extremes, you would not be acting like the partisans in this debate. They yearn for technological perfection in ways that will be described in Part I. Those in the privacy-enhancing camp wish for perfect, easy-to-use, easy-to-install programs that reveal the least amount of information necessary and use robust encryption to keep data away from third parties.[23]

Advocates on the other side want perfect transparency.[24] They believe that encryption should be limited to extreme situations, crippled with backdoors, or perhaps banned. The government should be able quickly and easily to access suspicious communications without encountering significant technological hurdles.

We should hope neither side gets what they want. There are problems with both types of perfection, which will be cataloged in Part II. Perfect transparency causes individual and societal harms that are well developed in the work of other scholars. Of specific concern are harms to the heroic dissident or freedom

---

[20] See Brad Templeton, *Is Strong Crypto Worse Than Weaker Crypto? Lessons from Skype*, Brad Ideas Blog (Aug 23, 2005), available at <http://ideas.4brad.com/node/263> (last visited Apr 3, 2008) (EFF board chairman arguing that Skype is important because it has placed encryption in the hands of many).

[21] Electronic Frontier Foundation, *EFF Joins Forces with TOR Software Project* (Dec 21, 2004), available at <http://www.eff.org/press/archives/2004/12/21-0> (last visited Mar 31, 2008) (describing EFF's involvement in the development of a privacy-enhancing technology known as The Onion Router, or TOR).

[22] Consider Louis Charbonneau, *Skype Encryption Stumps Police*, NZ Herald online (Nov 23, 2007), available at <http://www.nzherald.co.nz/section/story.cfm?c_id=5&objectid=10477899> (last visited Apr 3, 2008) (describing problems the German police are having wiretapping Skype-encrypted conversations); David S. Bennahum, *Can They Hear You Now? How the FBI Eavesdrops on Internet Phone Calls (and Why It Sometimes Can't)*, Slate (Feb 19, 2004), available at <http://www.slate.com/id/2095777> (last visited Apr 3, 2008) (discussing difficulty of wiretapping Skype calls).

[23] See Part I C.

[24] See id.

fighter who would risk being detected, identified, monitored, and silenced if he could not communicate privately. Unless he can find and use tools that allow him to communicate privately, he will be silenced.

The problem with perfect privacy is less well developed. Most obviously, perfect privacy enables undetected crime and unaccountable criminals. One man's criminal, however, is another man's freedom fighter, and there is no technology on Earth that will help or hinder one without doing the same for the other.

Less intuitively, perfect privacy will be met with direct, forceful, and most likely effective government countermeasures, also discussed in Part II. Once enough people can communicate privately using encryption, governments will pass new, increasingly draconian laws to try to ferret out wrongdoers in other ways, ironically causing more (and different) harms to privacy than those that the tools help avoid. Perhaps worse, government agents will come up with work-arounds: gray-hat surveillance that we should not want the government to fund or pursue.

Instead of perfection, this Article argues for "struggle": privacy and transparency-enhancing technology should require the privacy or transparency-seeker to struggle to achieve what they seek. Imperfection that leads to struggle avoids the problems with perfection.

In reality, we are unlikely ever to achieve technological perfection, so in one sense this Article is merely a thought experiment. Nevertheless, the debate between security and privacy has been pitched in the past, and the advocates have aimed for extreme positions. The hope is that recognizing the problems with perfection will quell desires for both perfect privacy and perfect transparency and encourage solutions aimed at struggle instead.

After abandoning hopes for perfection, in Part III, the Article asks to what level of technology should we aspire? Even if we abandon the endpoints—perfection of either sort—we will face a sliding scale of varying amounts of transparency and privacy. These amounts are easier to compare and consider when we replace the metaphor of the scale with a model of technological privacy (or transparency) that spans two dimensions, one that measures technical robustness and the other that measures user cost. One such two-dimensional model will be introduced and used to analyze different technologies.

Lastly, in Part IV, the Article will offer some thoughts about where on this two-dimensional graph we should reside—how much struggle is enough? It will propose that technology should

make it hard but possible for everybody to get what they want. Freedom fighters and criminals should be able to communicate privately, but only with effort. Likewise, the police should be able to find those they seek, but not too easily.

I. TECHNOLOGICAL TRANSPARENCY AND PRIVACY

First, a few definitions are needed. For this discussion, privacy means control over personal information.[25] Privacy also includes secrecy,[26] and in particular the secrecy of communications. These are imperfect definitions, chosen to reflect the particular and narrow nature of technologically-provided privacy and transparency, and not in an attempt to pick sides in the long-running debate about how to define privacy.[27]

Transparency means the absence of privacy. Put together with the previous definitions, transparency describes the lack of control over personal information, or an absence of secrecy. Transparency, as a value, is closely related to surveillance, the act that transparency enables. Surveillance is conducted by the state, by individuals, and by institutional actors, and although this Article focuses on the state, its conclusions apply to all actors. Because surveillance, however, has a negative connotation, I use transparency instead to reflect that transparency—just like privacy—is a quality that people often celebrate and desire. By definition, these two terms are complementary. As privacy increases, transparency decreases, and vice-versa.

Online, privacy usually takes one of three overlapping forms. First, online privacy means the *secrecy of personal data* such as the contents of communications. It means that people cannot access data and files belonging to others, neither while the data travels from source to destination nor when they are stored on computers and in online accounts. Second, online privacy means the *inaccessibility of the transactional records* of online behavior. Thus, people cannot tell when others are logged in, how many messages they send or receive, who they regard as friends, or

---

[25] See Alan Westin, *Privacy and Freedom* 7 (Atheneum 1967) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); Charles Fried, *Privacy*, 77 Yale L J 475, 482–83 (1968).

[26] See Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal L Rev 1087, 1105–06 (2002) (classifying secrecy as one aspect of a broader conception of privacy).

[27] See William M. Beaney, *The Right to Privacy and American Law*, 31 L & Contemp Probs 253, 255 (1963) ("[E]ven the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right.").

which provider they use. Third, online privacy describes the state of having online acts unlinkable to real-world identity or other acts. *Pseudonymity* is another word for this last aspect of privacy, and in the extreme case, it is called *anonymity*. Online transparency means the converse of these three forms.

A. Tools of Online Transparency and Privacy

The tools that are the subject of this Article are pieces of software that make a person's online activities either more transparent or more private.[28]

1. Transparency.

On the Internet, transparency is the technological default. Consider what most web browsers—such as Internet Explorer or Mozilla Firefox—expose to the world.[29] Every time a user uses a browser to visit a web page, say http://aljazeera.net, personal information is exposed in two ways. First, the web browser (in combination with the computer and operating system) reveals a lot of information about the user to other computers known as web servers.[30] In our example, the user's web browser tells the web server for aljazeera.net that the user's computer has a particular IP address,[31] that the user is using a particular type and version of web browser, that he prefers to read versions of web pages written in a particular language, say English or Arabic, and many other things.[32] Almost always, some of this incoming information is stored on the aljazeera.net web server, allowing human operators to review, summarize, use, and disclose the information to others.[33]

---

[28] Other scholars have referred to tools like these as "privacy-enhancing technologies," usually attributing the term to an article by Herbert Burkert. Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, in Philip E. Agre and Mark Rotenberg, eds, *Technology and Privacy: The New Landscape* 125 (MIT 1997). I am avoiding using that term because Burkert uses it to refer to "technical and organizational concepts that aim at protecting personal identity." Id. My focus is solely on technical, not organizational, concepts.

[29] See R. Fielding et al, *RFC 2616: Hypertext Transfer Protocol—HTTP/1.1* Ch 14 (1999), available at <http://www.ietf.org/rfc/rfc2616.txt> (last visited Apr 3, 2008) (section of formal definition of web transfer protocol describing "Header Field Definitions").

[30] Id.

[31] An IP address is a numeric identifier assigned to every computer on the Internet which is usually—although not always—uniquely identified with each individual computer.

[32] Fielding, *RFC 2616* (cited in note 29) (enumerating http headers).

[33] See Lee Tien, *Architectural Regulation and the Evolution of Social Norms*, 7 Yale J

Second, the communications sent or received while web browsing are sent *in the clear*.[34] Eve, using a computer connected in the path between the two communicating computers, could eavesdrop on this conversation and learn that somebody at a particular IP address visited aljazeera.net, surfed to particular pages on the aljazeera.net website, and entered particular text into the fields of the search boxes and other text fields of that website.[35]

Computer programmers often implement transparency not in conscious opposition to privacy, but because transparency is the default; it is what one gets when one does not think about privacy at all. The very essence of a network is the transfer of information between places, and therefore, unconscious programmer choices lead directly to transparency. In contrast, privacy requires conscious choice and specific implementation.

In addition to the inherent, default transparency of the Internet, many tools are designed to force transparency in situations that would otherwise involve privacy by enabling online surveillance. In the prior example, Eve probably used a packet sniffer, a tool that enables a computer to monitor communications flowing across a particular point on a network.[36] If a packet sniffer were connected to a main traffic hub on the network, it could collect the communications of dozens, maybe even hundreds or thousands of computers.

2. Privacy.

Good privacy online usually comes from encryption. Encryption refers to techniques that alter information using a secret code to make the information unintelligible to those lacking the code.[37] Importantly, there are three different ways in which software can use encryption to protect privacy online. First, encryption is used as it is in Skype, to protect communications "in flight" from point A to B. Typically, these tools use so-called en-

---

L & Tech 1, 12 (2004–05) (The popular Apache web server, "by default, records those who visit a website and post information.").

[34] "In the clear" is a term of art which means without encryption. See Neil Daswani, Christoph Kern, and Anita Kesavan, *Foundations of Security: What Every Programmer Needs to Know* 204 (Apress 2007).

[35] See Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw U L Rev 607, 649–51 (2003) (discussing tools known as packet sniffers used to capture network communications in real time).

[36] Id.

[37] Bruce Schneier, *Applied Cryptography* 1 (Wiley 1996).

crypted or secure tunnels, names metaphorically describing the way they surround communications in layers of encryption.[38] In this Article, this style of technological privacy will be called *tunnel privacy*.

Other tools encrypt data "at rest." These tools can be used, for example, to protect the privacy of files kept on a hard disk; information stored on a portable flash drive; or e-mail messages stored on a provider's computer.[39] This will be referred to as *endpoint privacy*.

Finally, some tools protect not the content of communication, but the identity of the person communicating.[40] This will be called *identity privacy*. Again, some of these tools use encryption, but many are far less complex. Anonymizing proxies, for example, are intermediary services that act like a trusted, privacy-obsessed Internet courier, visiting the websites users ask them to visit, refusing to divulge to third party computers any accurate information about the users or their computers, and forwarding content back to the users' computers.[41]

B. The Transparency-Privacy Spectrum and the Arms Race

Tools are typically regarded to provide a specific level of privacy or transparency measured along a spectrum.[42] Part III will strongly criticize this metaphor, but let us put aside its flaws for now. The endpoints of the spectrum are perfect transparency and perfect privacy. Between the endpoints, the level of one value decreases as the level of the other increases, due to the complementary nature of privacy and transparency.

Imagine that each computer program could be assigned a numeric grade from one to ten: ten meaning it would provide per-

---

[38] See Evi Nemeth, Garth Snyder, and Trent R. Hein, *Linux Administration Handbook* 708–710 (Prentice Hall 2007).

[39] See id at 696–97 (describing PGP).

[40] See Lorrie Faith Cranor, *Web Privacy with P3P* 36–39 (O'Reilly 2002).

[41] See id at 36–37. There is a vulnerability to this type of anonymization: although the website cannot trace the identity of the visitor, the anonymous proxy itself knows something more about the user. This is why proxies set up like this tend to have a policy of refusing to store records about their users. But see Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 497 (Academic 2d ed 2004) (quoting administrators of anonymous proxy service known as SafeWeb that logfiles were kept for seven days).

[42] See, for example, Lauren D. Adkins, Note, *Biometrics: Weighing Convenience and National Security against Your Privacy*, 13 Mich Telecomm & Tech L Rev 541, 552 ("If a sliding scale is used, gait, as compared with an iris, retinal scan or facial scan . . . would fall on the lower end of the spectrum.").

fect privacy, one signifying perfect transparency. A well-designed file encryption program might score a ten, for example; a flawed tunnel encryptor might score a five; and an email program that uses no encryption, a one.

For any given computer a collective grade can also be computed, perhaps by summing, or averaging, or calculating the median of all of the scores for all the programs on the computer.[43] Over time, a computer's grade will change. Sometimes, the grade will shift a lot, for example lurching toward a better privacy score when the computer's administrator installs a firewall or shifting toward a better transparency score when a major new operating system vulnerability is first discovered.[44] More often, the grade will move in smaller steps, with new software nudging the score one way or the other.

We can already begin to see the problems with reducing privacy and transparency to a single score because this one-dimensional approach masks a diverse set of measurements. A score of five might mean that a user's computer would provide significant tunnel privacy—the user might always connect through an encrypted tunnel provided by his employer, for example—while allowing for complete endpoint transparency—the user might have inadvertently shared the contents of his unencrypted disk with thousands of users of a peer-to-peer network.[45] Alternately, five might mean the computer would provide average privacy across the board.

Some see computer software marching inexorably toward better privacy[46] or transparency.[47] This is not unusual, as tech-

---

[43] Because this is a thought experiment, the details are not important. One should assume that such a score could be calculated, but the method of computation need not be specified. This is also the reason that other complexities can be ignored. For example, an operating system is a massive computer program with hundreds, maybe thousands of different privacy-related functions. For this discussion, the reader should simply assume that the operating system's score can be computed as an aggregate score of the program.

[44] SANS, *Top-20 2007 Security Risks (2007 Annual Update)*, available at <http://www.sans.org/top20/> (last visited Apr 3, 2008) (listing critical vulnerabilities).

[45] See Grant Gross, *P-to-P Users Expose U.S. Government Secrets*, PC World Online (July 27, 2007), available at <http://www.pcworld.com/article/id,135167-page,1/article.html> (last visited Apr 3, 2008) ("Contractors and U.S. government employees are sharing hundreds of secret documents on peer-to-peer networks, in many cases overriding the default security settings on their P-to-P software to do so, according to a company that monitors the networks.").

[46] See David Stoll, *A Comment on the Encryption Debate*, 1998 Stan Tech L Rev 1 ("The real reason encryption regulations will not work is that no government alone, not even the United States, can prevent the inevitable spread of stronger and stronger forms of encryption."); Froomkin, 1996 U Chi Legal F at 69 (cited in note 5) (noting the National Research Council's conclusion that "widespread cryptography is inevitable"); National

nology's progress is often imagined as a march or evolution in a particular direction, embodied both literally and metaphorically in rail lines crossing the continent and telegraph wires submarining across the ocean.

The problem with this vision is that privacy and transparency are developed by two camps of programmers locked in an arms race,[48] as is often the case with software conflicts. Developers of tunnel encryption tools try to give users greater privacy, while developers of packet sniffers provide better transparency. At any given time, one side holds the upper hand, but the inherent arms race makes the war tend toward stalemate, or at least makes it very difficult to predict a winner.[49] The arms race model also focuses solely on the effect of changes internal to the racing parties. It ignores unexpected outcomes and negative externalities.

In fact, many important software developers develop for both sides of the arms race, pushing further toward stalemate. Manufacturers of operating systems, for example, sometimes choose privacy—installing disk encryption tools by default, for example—and sometimes choose transparency—such as keeping disk encryption turned off by default—usually eschewing privacy in the name of efficiency or ease-of-use.

Because of the arms race, our tools are usually far from perfect. One would not know this, however, by listening to the bluster of the advocates in the field.

Research Council, Kenneth Dam and Herb Lin, eds, *Cryptography's Role in Securing the Information Society* 22–50 (National Academy 1996).

[47] See Bert-Jaap Koops and Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 Mich Telecomm & Tech L Rev 115, 177 (2005) ("The eroding effect of technology on privacy is thus a slow, hardly perceptible process. There is no precise stage at which one can stab a finger at technology to accuse it of unreasonably tilting the balance of privacy."). See also Brin, *The Transparent Society* at 8–9 (cited in note 8) ("The *djinn* cannot be crammed back into its bottle. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay.").

[48] Consider Lee Kovarsky, *A Technological Theory of the Arms Race*, 81 Ind L J 917 (2006) (discussing arms races); James Grimmelmann, *The Structure of Search Engine Law*, 93 Iowa L Rev 1, 13–14 (2007) (discussing the arms race between search engines and search engine optimization firms).

[49] See Brin, *The Transparent Society* at 282 (cited in note 8) ("I asked Whitfield Diffie if he felt that . . . the outcome of the [encryption] arms race was a foregone conclusion. Had the advantage been permanently settled in favor of the encryptor, over some team of well-equipped math wizards trying to break another person's code. Diffie's answer surprised me: 'No, I can't say any such thing. I don't think that's been decided at all.'").

C. The Quest for Perfection

No technology is perfect, and advocates who comment on privacy and technology in truth almost never advocate for perfect privacy or perfect transparency. But these advocates clearly strive for something close to perfection.[50] Perfection, as used throughout this article, refers to technology that works flawlessly according to design.[51] For privacy advocates, the goal is widespread encryption, unfettered by government backdoors.

For example, Marc Rotenberg, an outspoken privacy advocate who heads the Electronic Privacy Information Center, has spoken out several times in favor of widespread encryption and against government policies he sees as thwarting that goal.[52] Attorneys for the Center for Democracy and Technology, have made similar comments.[53]

The Electronic Frontier Foundation ("EFF") has expressed its support for widespread, easy-to-use cryptography more often through actions, not words. In 1997 and 1998, for example, EFF funded a project to build a device capable of cracking the DES encryption protocol. They did this to demonstrate how the government's approved standard for encryption was vulnerable to

---

[50] The brief sketches that follow are necessarily incomplete, as these various organizations have many other pressing concerns aside from technological privacy and transparency. By omitting some of the nuances of their positions, there is a risk of caricature. Also, individuals in these organizations no doubt hold more subtle, complex views about these questions. Nevertheless, these groups hold themselves out, institutionally at least, as committed to a march toward perfect technology.

[51] As will be elaborated in Part III, perfection assumes the absence of user error.

[52] See, for example, Security and Freedom Through Encryption (SAFE) Act, Hearing on HR 695 before the House Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, 105th Cong, 1st Sess (Mar 20, 1997) (statement of Marc Rotenberg, director of the Electronic Privacy Information Center), available at <http://www.fas.org/irp/congress/1997_hr/h970320epic.htm> (last visited Apr 3, 2008) ("It would be foolhardy for our government not to anticipate that strong, unbreakable encryption will be widely available on the Internet. And it would be equally wrong to prevent American citizens and American businesses from making use of the best tools available to protect their sensitive information from potential criminal threats.").

[53] See, for example, Wireless Privacy Enhancement Act of 1999 and the Wireless Communications and Public Safety Enhancement Act of 1999, Hearing on HR 438 and HR 514 before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, 106th Cong, 1st Sess (Feb 3, 1999) (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology), available at <http://www.cdt.org/testimony/19990203dempsey.html> (last visited Apr 3, 2008) ("The current policy of government controls on encryption will not work in the decentralized, competitive, global environment where criminals will always be able to obtain strong encryption to shield their communications. The sooner strong encryption is widely deployed in wireless systems for the rest of the population, the sooner privacy will be protected and fraudulent theft of services will be curtailed.").

inexpensive circumvention.[54] Later, EFF sponsored the developers of privacy-enhancing software known as The Onion Router, or "TOR."[55]

Many computer scientists share the view that widespread encryption is good, even imperative. Whitfield Diffie and Susan Landau, for example, claim to argue for less than "an absolute right of private conversation," not because such a right would be unwelcome, but because it would be "doomed to failure."[56] Still, their hopes lie in perfection because they see good encryption as the way to "restore some of the privacy lost to earlier technological advances,"[57] restoring us to the level of privacy held by our agrarian forebears.[58] In particular, "ubiquitous use of cryptography" is the best choice in their minds because the police will be able to work around it[59] and the "wide dissemination of high-grade cryptography" could be undone if policymakers realize that it turns out to be a mistake.[60]

Next, consider calls for perfect transparency. Although the government has not often spoken publicly about encryption in the past decade, various government agencies have taken positions that, at their core, advocate perfect transparency. Most notable is the government's advocacy for the Clipper Chip and a law called the Communications Assistance for Law Enforcement Act ("CALEA").[61]

CALEA was passed in 1994[62] to combat law enforcement's fears that it was losing the wiretapping arms race.[63] As more people moved away from land-line telephones to cell phones and

---

[54] Electronic Frontier Foundation, *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design—How Federal Agencies Subvert Privacy* available at <http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/19980716_eff_des.faq> last updated Jul 16,1998 (last visited Apr 3, 2008).

[55] See Electronic Frontier Foundation, *EFF Joins Forces with TOR* (cited in note 21).

[56] Diffie and Landau, *Privacy on the Line* at 9 (cited in note 3).

[57] Id at 4.

[58] Id at 128 ("Three hundred years ago . . . [e]avesdroppers were easily avoided by walking to a place where one could not be overheard.").

[59] Id at 242.

[60] Diffie and Landau, *Privacy on the Line* at 244 (cited in note 3).

[61] Communications Assistance for Law Enforcement Act, Pub L No 103-414, 108 Stat 4279, codified at 47 USC § 1001 et seq (1994).

[62] Id.

[63] Froomkin, 143 U Pa L Rev at 743–44 (cited in note 5) ("In its hard sell, the Administration, primarily through the FBI, paints a lurid picture of law enforcement stripped of an essential crime-detection and evidentiary tool—wiretapping—while pornographers, drug dealers, terrorists, and child molesters conspire via unbreakable ciphers, storing their records and child pornography in computers that become virtual cryptographic fortresses.").

the Internet, law enforcement worried that, even armed with court-issued warrants, it would encounter providers who would not be able to tap a particular type of line or isolate a particular type of communication.[64] In other words, the police feared that the balance between privacy and transparency was tipping quickly toward too much privacy, and not enough transparency.

The solution was an elaborate new law, administered by the Federal Communications Commission, which tips the scales dominantly back toward security interests. Each provider—every phone company and ISP—is obligated to "ensure that its equipment, facilities, or services . . . are capable of expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept . . . all wire and electronic communications carried by the carrier within a service area."[65]

The FCC has interpreted CALEA broadly. The FCC has ruled that, under CALEA, providers are required to provide police access to the contents encrypted in VoIP systems and the packets traveling through switches in an Internet provider.[66] In other words, providers cannot deploy privacy-enhancing technologies unless they ensure "backdoor" access to the contents of the communication.

CALEA forces programmers to build transparency into software in some situations when developers might have otherwise chosen privacy.[67] It is a typical example of how law has been used to try to bring about perfect transparency. Law enforcement's concerns about a tilt of its investigative playing field were met with a drastic tilt in the opposite direction.

---

[64] Telecommunications Carrier Assistance to the Government, HR Rep No 827-103, 103rd Cong 2d Sess 12–13 (1994) ("[I]t became clear to the Committee early in its study of the 'digital telephony' issue that a third concern now explicitly had to be added to the balance, namely, the goal of ensuring that the telecommunications industry was not hindered in the rapid development and deployment of the new services and technologies that continue to benefit and revolutionize society.").

[65] 47 USC § 1002.

[66] Federal Communications Commission, *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Second Report and Order and Memorandum Opinion and Order, FCC 06-56 (May 3, 2006).

[67] Some might object that it is difficult for law to influence technology. I disagree with this proposition, but I will not develop my argument now. Instead, this Article adopts as a premise that technology should be seen as controllable and contingent. Whether or not technology should be changed to accommodate policy goals, it can be changed, and I start from that assumption. The task is to investigate when law should be allowed to push technology to make it less privacy-protective, if ever at all.

Similarly, the Clipper Chip would have provided the government with flawless backdoor access to private communications. Government officials have emphasized how neither CALEA nor Clipper allow unrestricted government access, because the government typically still must use a court order to take advantage of either.[68] For purposes of this article, however, this argument is not responsive because promises to use court orders and warrants can later be withdrawn.[69] With both CALEA and Clipper, the government tried to enable perfect technological transparency.

Both of these government responses tried to shift from perfect privacy—resulting from troublesome hardware in the case of CALEA, and encryption in the case of Clipper—all the way to perfect transparency by forcing conditions that would have allowed unencumbered wiretapping.

The FBI demonstrates its desire for transparency not only through laws and policies, but also in words. In most cases it frames the debate as a matter of life and death. Arguing for the Clipper Chip, FBI Director Louis Freeh made countless public predictions about the grave danger of widespread encryption. "Advanced technology will make it impossible for the FBI to carry out court-approved surveillance in life-and-death cases."[70] The FBI often invoked the specter of terrorists—pre 9/11—or harm to children.[71] The two themes came together in quotes like, "I doubt that Congress would pass on the opportunity to make sure that our children were safe from terrorists."[72]

D. Arms Stockpiling in the Decade Since Clipper

Most of the quotes in the previous Part were uttered during the very public, bruising debate about the Clipper Chip in the early 1990s. That debate gave way to a subsequent decade of

---

[68] See *Question 19, Are FBI Special Agents Permitted to Install Wiretaps at Their Own Discretion?*, Communications Assistance for Law Enforcement Act AskCALEA, "Frequently Asked Questions", available at <http://www.askcalea.net/faq_answers/019_faq.html> (last visited Apr 3, 2008) (stating that FBI agents are not permitted to install wiretaps without court order).

[69] See Froomkin, 143 U Pa L Rev at 762–63 (1995) (cited in note 5) ("The Attorney General's [Clipper key escrow] procedures themselves are merely directives. They are not even legislative rules, which might be subject to notice and comment restrictions before being rescinded.").

[70] Froomkin, 143 U Pa L Rev at 746 n 151 (cited in note 5).

[71] Id at 743–44.

[72] Electronic Frontier Foundation, *EFF Quotes Collection* 19.6 (Apr 9, 2001), available at <http://w2.eff.org/Misc/EFF/?f=quotes.eff.txt> (last visited Apr 4, 2008).

surprising silence. There have been a few public squabbles, most notably the FBI's moves to expand the interpretation of CALEA in FCC rulemaking and the privacy community's mostly failed attempts to rebuff those interpretations. In 2004, the FBI filed a petition with the FCC—the agency given interpretative rulemaking power under the law—to interpret CALEA to cover not only digital telephone networks but also broadband Internet networks and VoIP calls.[73]

But the most striking, and until now mostly unobserved, developments have been in the technological arms race, as new tools that can bolster or pierce privacy continue to be created and deployed by parties on all sides.

Programmers continue to improve encryption, making it increasingly available to the masses. Skype is not the only example of seamless, invisible privacy that users enjoy by default. A tunnel encryption technology known as Secure Sockets Layer ("SSL")[74] is shipped with every modern web browser; although most users probably do not know SSL by name, many know that the little lock icon in their browser (which represents an SSL connection) signifies protected privacy. Many users of BitTorrent, a peer-to-peer protocol useful for transferring large files, use tools that encase data within encrypted tunnels.[75]

Developers are incorporating encryption not only to create tunnel privacy, but also to protect the *stored* files of the masses. For example, Microsoft has created two complementary systems, BitLocker and encrypted file system ("EFS"), that together encrypt data stored on hard drives.[76] If these technologies were to become widespread, the FBI would have grave difficulties analyzing seized computers.[77] Perhaps responding to law enforcement's concerns, Microsoft has chosen not to provide this tech-

---

[73] Federal Bureau of Investigation and Drug Enforcement Administration, *In the Matter of United States Department of Justice*, Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, Mar 10, 2004, available at <http://www.cdt.org/digi_tele/20040310fbipetition.pdf> (last visited Apr 4, 2008).

[74] Alan O. Freier, Philip Karlton and Paul C. Kocher, *The SSL Protocol, Internet Draft* (Mar 1996), available at <http://tools.ietf.org/html/draft-freier-ssl-version3-01> (last visited Apr 4, 2008).

[75] See note 191 and accompanying text.

[76] Jamie Morris, *Notes on Vista Forensics, Part One*, SecurityFocus (Mar 8, 2007), available at <http://www.securityfocus.com/infocus/1889> (last visited Apr 4, 2008).

[77] Id.

nology to every Windows user, limiting the spread of the technology, and hence the FBI's grief.[78]

On the other side, developers of tools that force transparency continue to improve their products, as well. The FBI spent much of the past decade tamping down the controversy about its packet sniffing, filtering tool known as Carnivore.[79] Despite the fact that, to some, Carnivore has become a stand-in for menacing technologies that the FBI and NSA can use to "eat" all of our private information, the technology was actually a relatively mundane packet sniffing and filtering system.[80] In 2005, reports surfaced that the FBI had stopped using Carnivore, turning to standard, off-the-shelf products instead.[81] If true, this move may have been motivated by the public controversy, but it is also likely that the FBI decided to get out of the sniffer-writing business because the private sector did it so well.

II. THE PROBLEM WITH PERFECTION

We should hope that we end up with a world of neither perfect transparency nor perfect privacy. There are significant harms that would result from either extreme. Those problems will be described in depth, but first consider the benefits of an alternative to perfection, what I am calling struggle.

A. Struggle

When policymakers weigh the tradeoffs between privacy and transparency they emphasize balance, perhaps imagining the need to fiddle with the volume knob on a stereo amplifier to find the perfect level. The experts advising them feed this imagery, fixated as they are on extreme positions: perfect privacy (turn the volume all the way up) and perfect transparency (turn the volume all the way down).

Privacy advocates want as much privacy as possible and the FBI wants perfect surveillance. Even when both sides are willing to concede the acceptability of something less than perfect, their

---

[78] Id (reporting that BitLocker is available in Vista Enterprise and Ultimate and EFS is available in the Business, Enterprise, and Ultimate editions).

[79] See Kerr, 97 Nw U L Rev at 651–54 (cited in note 35).

[80] Id at 654.

[81] Xiaomin Huang, Peter Radkowski, III, and Peter Roman, *Computer Crimes*, 44 Am Crim L Rev 285, 324 n 326 (2007) available at <http://www.securityfocus.com/news/10307> (last visited Apr 4, 2008) (citing Kevin Poulsen, *FBI Retires Its Carnivore*, SecurityFocus (Jan 14, 2005)).

concessions tend to hover near the extremes, coming nowhere near balance. If ten is perfect privacy and one is perfect transparency, privacy advocates might concede that privacy should sometimes give way when lives are in danger, an eight or a nine, but in no other situations. Likewise, the FBI might concede that communications between attorneys and clients should be very difficult to pierce, but it would never accept anything above two or three. The policymaker aiming for five will be steered away from potentially good but imperfect solutions by both sides.

Instead of balance, policymakers should embrace a different metaphor—struggle. Transparency and privacy should come only with struggle, only at a cost. It should be difficult for speakers to attain robust, easy privacy, and it should be hard for eavesdroppers to force seamless, easy transparency.

To understand why struggle is better (or even different) than balance, think about the limitations of the balance metaphor. Things in balance tend to be unstable. The arms of a scale, a tightrope walker, even a checkbook—these things teeter precariously when balanced, and without constant attention, they fall out of balance.

Struggle inverts the usual analysis, thereby avoiding many of the problems that result from tiptoeing along the tightrope. Struggle is a negative value, defined by what it is not. It is not a statement of where we should be along the spectrum; it instead describes where we should *not* be, at the extreme ends. Perfect privacy and perfect transparency should both be avoided.[82]

Historically, the technological status quo has ensured struggle, so we have not had to think about it. Consider cash. Cash is often mythologized in legal scholarship as a technology of perfect anonymity.[83] But cash does not provide perfect anonymity. Many

---

[82] So long as privacy and transparency are seen as sitting along a one-dimensional spectrum, struggle suffers from some of the same problems as balance—a little struggle is never enough. We will return to these problems in Part III, but the important point for now is that struggle is a better goal than balance for finely calibrating the power relationship between the government and criminal targets.

[83] As a typical example:

> The simplest means of facilitating anonymity is the use of cash, as opposed to credit or other smart card devices. Payment with cash does not require verification of credit or identity, and the name of the purchaser is not registered. Thus, no link is formed between the participant in the transaction and his actual identity or other patterns of behavior. Cash, therefore, is the basic "anonymizer."

Tal Z. Zarsky, *Thinking outside the Box: Considering Transparency, Anonymity, and Pseudonymity As Overall Solutions to the Problems of Information Privacy in the Internet*

criminals are caught despite having used cash in their crimes. Cash is an imperfect technology for privacy. Its value is realized only through transfer, yet transfers also generate the risk of discovery. A drug buyer might snitch; a merchant selling a pre-paid cell phone might remember the buyer's physical description. Cash can be booby-trapped or seeded with traceable serial numbers.[84]

Instead of perfection, cash ensures investigatory struggle. It is not easy to investigate criminals using cash. Cash forces the police to engage in expensive operations. Compare the struggle introduced by cash to the near-perfection possible with the software tools described in this article. These tools have the potential to tip the investigative playing field so much, they introduce risks and fears rarely encountered in transactions occurring entirely within the physical world.[85]

To understand why perfection is dangerous and struggle is necessary, consider the following pair of thought experiments about the consequences of zero struggle at opposite ends of the privacy-transparency spectrum: what problems arise when the police can surveil too easily or when speakers can communicate without detection?

B. The Problem with Perfect Transparency

Perfect transparency silences people struggling against their governments, those known as freedom fighters or dissidents (depending on one's point of view).[86] When a dissident's online communications and identity are transparent, government agents

---

Society, 58 U Miami L Rev 991, 1026 (2004). But see A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J L & Comm 395, 472 (1996) ("[I]t should be noted that paper money is not as anonymous as it may seem.").

[84] Froomkin, 143 U Pa L Rev at 727 n 58 (cited in note 5) ("U.S. paper money is not completely anonymous, however, because each (authentic) bill carries a unique serial number and bills can be marked to facilitate tracking.").

[85] Id at 817–18 ("Cryptography allows unprecedented anonymity both to groups who communicate in complete secrecy and to individuals who, by sending electronic mail through anonymizing remailers, can hide all traces of their identity when they send mail to other persons.").

[86] Although the phrase "freedom fighter" conjures most easily the image of the protestor living in a totalitarian state, of course, dissidents live in every nation. No matter the form of government, states throughout history have tried to monitor their dissidents, to greater or lesser extent. In the United States, for example, the history of wiretapping has been checkered and problematic. See Diffie and Landau, *Privacy on the Line* at 137–48 (cited in note 3) (cataloging abuses of wiretapping by American law enforcement from the 1940s to the 1990s).

can monitor his communications, rifle through his stored files, and attribute pseudonymized speech to him.[87] These acts specifically deter dissidents, by allowing them to be harassed or imprisoned, and generally deter others by creating the fear that if they too dissent, they will be watched. In a world of too much transparency, perhaps it is simply best not to dissent.

Even for non-dissidents, transparency leads to a long list of individual and societal harms, which have been well documented by other scholars.[88] A world of perfect surveillance would be a world where the police could chip away at individual dignity and autonomy.[89] It would be a world where we would never be able to remove our external masks, and we would lose the ability to "try out" different personas, to develop into who we would want to become.[90] In short, surveillance, made possible by transparency, strips the individual of dignity, autonomy, a sense of repose, and the capacity for self-determination.[91]

---

[87] Froomkin, 143 U Pa L Rev at 820 (cited in note 5) ("Groups seeking to change the social order in ways likely to be resented by the police and others in positions of power will have reason to fear that state actors will find ways to access their [cryptographic] keys.").

[88] See, for example, Solove, 90 Cal L Rev at 1099–1126 (cited in note 26); Paul M. Schwartz, *Internet Privacy and the State*, 32 Conn L Rev 815, 818–19 (2000); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan L Rev 1193, 1212–17 (1998).

[89] These value are usually captured under the umbrella value, the protection of personhood. The idea of privacy relating to personhood is often traced back to Paul Freund, who defined personhood as "those attributes of an individual which are irreducible to selfhood." American Law Institute, 52nd Annual Meeting 42 (1975); Solove, 90 Cal L Rev at 1116 (cited in note 26).

[90] Kang, 50 Stan L Rev at 1219–20 (cited in note 88) ("The ability to maintain divergent public and private personae creates the elbowroom necessary to resist social and political homogeneity.").

[91] Although this Article describes the connection between technology and some significant harms, some of these harms turn not on the amount of privacy we *have*, but depend instead on the amount of privacy we *think* we have. Take the harm to an individual's sense of repose. One loses repose when he worries that he is being watched, regardless of whether anybody is watching. The reverse is also true: the person who is continuously watched can still find repose, so long as he mistakenly thinks he has privacy. Tools which increase privacy decrease the harm to the sense of repose only if the user understands what the tool can do. In this sense, then, some of these harms are remediable only through public education, not through tools.

Similarly, the government will often overreact to the threat or promise of future privacy-enhancing technology, even when the reality is much less threatening. Very often, law enforcement officials press for legislative change, spurred by fears of potential power, even if they cannot prove that the power is being used. I explored this type of response, which I call the Myth of the Superuser, in another article. Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 UC Davis L Rev 1327 (2008). Because the Myth so often rests on questionable empirical evidence, I have argued that policymakers should rarely act if the only evidence of a looming problem are unsupported claims of potential online power. Id at 1393–96.

Others value privacy for properly calibrating the relationship between the person and the state. It prevents a "creeping totalitarianism, an unarmed occupation of individuals' lives."[92] Some see it as giving us the space for the development of intimacy.[93] A final group of scholars, branded by some as part of a "New Privacy" movement,[94] go a step farther, looking past harms to individuals from insufficient privacy, and arguing instead that the result of these individual harms is a loss to society generally.[95] For example, robust democratic deliberation itself requires the privacy to speak freely and experimentally, to try out new ideas.[96]

C. The Problem with Perfect Privacy

The problems with perfect privacy have been discussed less by scholars. In a world with perfect privacy, evildoers—including garden-variety computer criminals, online terrorists, and enemy soldiers—would have an easier time acting with impunity. Truly anonymous speech would protect the identities of (and prevent detection of possible planning by) those who send death threats, blackmail, and conspiratorial messages.[97]

This is an important—albeit often exaggerated—harm, but it is so intuitive as to need little elaboration. We know that bad people will take advantage of technological privacy; what other concerns arise? Consider two significant yet underappreciated harms resulting from the ways powerful entities—and in particular governments—would *react* to perfect privacy.[98] These powerful entities, threatened by technological privacy,[99] would launch *countermeasures* causing significant and underappreciated

---

[92] Jed Rubenfeld, *The Right of Privacy*, 102 Harv L Rev 737, 784 (1989)

[93] Julie C. Inness, *Privacy, Intimacy, and Isolation* 74–94 (Oxford 1992).

[94] Paul M. Schwartz and William M. Treanor, *The New Privacy*, 101 Mich L Rev 2163, 2177 n 33 (2003) (listing legal publications on "New Privacy").

[95] Schwartz, 32 Conn L Rev at 834 (cited in note 88) ("Put simply, access to personal information and limits on it help form the society in which we live in and shape our individual identities.").

[96] See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand L Rev 1609, 1653–58 (1999).

[97] There are other, lesser concerns, such as identifying those who post defamatory messages or those who illegally traffic in copyrighted materials.

[98] The focus of the following is on government countermeasures. Powerful private sector players may engage in some of these types of countermeasures as well.

[99] Of course, powerful entities would benefit from increased privacy, too. Nevertheless, I predict that the threat will spur these entities to act, even if it means reducing their own access to technological privacy.

harms. These underappreciated harms are as significant as the threat of undetectable crime.

1. Government countermeasures I: new legislation.

The police would likely tell compelling and convincing stories of the potential for undetectable crime to judges and legislators to support calls to change or reinterpret the law, perhaps in the wake of some future attack.[100] Courts and Congress might respond by sanctioning new tools and techniques and by relaxing civil liberties.[101] These laws would likely take one of two forms. First, they may, like CALEA, target the developers of privacy-enhancing technologies, forcing them to reengineer their systems to make them more vulnerable to law enforcement demands. Second, these laws might target the people communicating, trying to force them to disclose their passwords or other security measures in the face of a law enforcement investigation.[102] In either case, these laws would be probably used frequently (maybe even exclusively) against people who are not using privacy-enhancing technology,[103] harming instead people who were not the original justification for the rule.

---

[100] Writing in the late 1990's, after the 1993 attack on the World Trade Center but before 9/11, David Brin made some chillingly prescient statements:

> As a mental experiment, let's go along with FBI director Freeh and try to envisage what might have happened if those bombers had actually succeeded in toppling both towers of New York's World Trade Center, killing tens of thousands. Or imagine that nuclear or bio-plague terrorists someday devastate a city. Now picture the public reaction if the FBI ever managed to show real (or exaggerated) evidence that they were impeded in preventing the disaster by an inability to tap coded transmissions sent by the conspirators. They would follow this proof with a petition for new powers, to prevent the same thing from happening again.
>
> Such requests might be refused nine times in a row, before finally being granted on the tenth occasion. The important point is that once the bureaucracy gets a new prerogative of surveillance, it is unlikely ever to give it up again. The effect is like a ratchet that will creep relentlessly toward one kind of transparency, the kind that is unidirectional.

Brin, *The Transparent Society* at 206–07 (cited in note 8).

[101] Id; Ohm, 41 UC Davis L Rev at 1348–57 (cited in note 91).

[102] See, for example, Adam Liptak, *If Your Hard Drive Could Testify . . .*, (cited in note 14) (describing court's holding that the government could compel a Canadian citizen named Sebastian Boucher to produce the password protecting his computer's files without violating his Fifth Amendment right against self-incrimination); Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U Chi Legal F 171.

[103] See also Ohm, 41 UC Davis L Rev 1349–52 (cited in note 91) (arguing how expansions to 18 USC § 1030's prohibitions on computer hacking are often used to prosecute unsophisticated actors).

2. Government countermeasures II: gray-hat surveillance.

Even more worrisome than changes to the law would be what I call gray-hat surveillance. The adjective comes from computer security jargon where "black hats" are people with unambiguously evil motives, "white hats" are the good guys, and "gray hats" fall in ethically murky areas in between.[104] I use gray-hat surveillance to describe an anticipated shift in police practices into the darker, more ethically murky areas of computer programming and surveillance.

Law enforcement agencies, and in particular the FBI, will feel pressure to build software tools to blunt the effect of better and more widespread privacy-enhancing software. Before describing why gray-hat surveillance is harmful, let us explore why it is useful for the police.

a) Privacy's analog hole. It may seem inconsistent on the one hand to imagine a world of "perfect" privacy-enhancing technology while on the other hand speaking about gray-hat surveillance which can defeat perfection. To resolve this seeming contradiction, we must sharpen what we mean when we say "perfect." Perfect privacy-enhancing technology tends to protect robustly but incompletely.

Consider encrypted tunnels again. Perfect encryption, by definition, cannot be pierced.[105] Thus, encrypted tunnel privacy makes it impossible for a person with access to a wire between the two communicating parties to wiretap the communication. In the case of the communications of suspected criminals, an encrypted tunnel renders the FBI deaf, but only when agents are sitting somewhere in the middle, on the wire. If instead the agents were to find a way to access the endpoints of the communication, they could grab messages as they were sent, before they have been wrapped in encryption, or received, after they have been decrypted.[106]

---

[104] Dean J. Champion, *The American Dictionary of Criminal Justice: Key Terms and Major Court Cases* 114, 267 (Roxbury 3d ed 2005) (definitions of "gray hat", "black hat," and "white hat").

[105] This discussion is focusing exclusively on ways around perfect technology. It is important not to forget also that if the technology is imperfect, attackers may find the vulnerabilities. See Brin, *The Transparent Society* at 285 (cited in note 8) ("Even if the keys are never cracked by brute force, the deciphering algorithm may be flawed, or compromised by some intentional or unforeseen 'back door.'").

[106] Even without ever listening to communications using the methods described in this subpart, the police can sometimes learn enough from the non-content attributes of a communication to identify or locate the speaker. This highlights the difference between tunnel and identity privacy. See Part I A 2.

Think of this like the privacy of a high fence with a gate. The fence prevents many privacy invasions: if it is solid, people cannot peer through it; if it is tall, people cannot climb it; if it is thick, people cannot eavesdrop through it. But as things travel through the gate, they can be intercepted just before they enter or as soon as they emerge, and privacy can thereby be breached. Legal scholars often err when assessing cryptography, focusing too much on how impossible it is to break—on the height of the fence—ignoring the other ways people can circumvent even good cryptography—by waiting at the gates.[107]

For example, if the FBI could somehow aim a hidden video camera at a target's computer screen or keyboard, it could track his communications, even if he were using an encrypted tunnel.[108] Better yet, the police could install a "key logger" on the target's computer.[109] Key loggers are software or hardware devices installed surreptitiously on a target's computer, which record every key pressed on the keyboard or snapshots or videos of everything that flits across the screen.[110]

The fact that a key logger can work despite the use of robust encryption can be thought of as privacy's version of the analog hole, a term that arises in the intellectual property debate over Digital Rights Management ("DRM"). DRM technologies are used

---

In 2006, tracking the non-content attributes of a communication helped the U.S. police find fugitive Kobi Alexander, former CEO of Comverse, who had fled to Sri Lanka after being indicted for defrauding his shareholders. Eric Bangeman, *Fugitive Exec Nabbed after Skype Call*, Ars Technica (Aug 24, 2006), available at <http://arstechnica.com/news.ars/post/20060824-7582.html> (last visited Apr 4, 2008). After Alexander placed a one-minute phone call from Skype, the authorities were able to trace him down (presumably through his IP address) and bring him back into custody. Id.

[107] See, for example, Ric Simmons, *Why 2007 Is Not Like 1984: Broader Perspectives on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J Crim L & Criminol 531, 546 (2007) ("[T]here is no type of responsive surveillance technology that can be used to counteract the greater privacy enjoyed by individuals (including criminals) who make a serious effort to encrypt their communications.").

[108] No doubt, the FBI is harnessing miniaturization as a way of getting cameras unobtrusively into private places. Consider Charlie White, *DelFly II, Just the First of a Long Line of Tiny Flying Robot Spycams*, Gizmodo (Nov 2, 2007), available at <http://gizmodo.com/gadgets/eye-on-you/delfly-ii-just-the-first-of-a-long-line-of-tiny-flying-robot-spycams-318161.php> (last visited Apr 4, 2008) (describing a robotic dragonfly with on board camera); Brin, *The Transparent Society* at 285–86 (cited in note 8) (describing the development of miniature cameras). Of course, if the government wanted to use such a camera to monitor a place where the people monitored had a reasonable expectation of privacy, it would require at least a search warrant under the Fourth Amendment. *People v Dezek*, 308 NW2d 652 (Mich App 1981) (holding that video surveillance of activity within stalls of public restroom is a Fourth Amendment search).

[109] *United States v Scarfo*, 180 F Supp 2d 572 (D NJ 2001) (describing investigation using key logger to intercept passwords).

[110] Id.

by the owners of content—such as music, movies, or software—to control how users can access the content. DRM, for example, might allow users to watch a movie on his desktop computer but would prevent him from copying the video to his laptop or distributing it across a peer-to-peer network.[111] The analog hole is an inherent vulnerability in DRM systems, arising from the fact that content can be captured as it is being listened to or viewed.[112] A movie or television show playing on a screen, for example, can be filmed by a video camera, resulting in a degraded-quality but watchable copy, unencumbered by DRM.[113]

Just as with DRM, technologically-provided privacy has an analog hole. Regardless of how encryption is used to protect the privacy of communications (be they in-flight, in storage, or used to anonymize identity) the communication must be created with a keyboard or output to a screen. If the government can take control of a user's keyboard or screen, it can take advantage of privacy's analog hole to defeat even the best encryption.[114]

b) The Timberline High case. The police exploit privacy's analog hole by borrowing the tricks of hackers, spyware creators, and virus writers. Consider a recently revealed example of police gray-hat surveillance.[115] The FBI could not have wished for more sympathetic facts to justify aggressive surveillance: the pursuit of the anonymous author of several email messages threatening to blow up Timberline High School, in Lacey, Washington.[116]

The anonymous messages were both chilling—going into great detail about where bombs would be placed—and taunting—repeatedly daring investigators to try to track the anonymized messages across the Internet.[117] The suspect had routed at least some messages through a computer in Italy, and the FBI had

---

[111] See Douglas C. Sicker, Paul Ohm, and Shannon Gunaji, *The Analog Hole and the Price of Music: An Empirical Study*, 5 J Telecomm & High Tech L 573, 574 (2007).

[112] Id at 576.

[113] Id at 577.

[114] See Brin, *The Transparent Society* at 220 (cited in note 8) ("[E]ncryption would have stymied hardly any of the surveillance techniques used by the Gestapo, or Beria's NKVD, let alone the far more advanced abilities that will be available in an age of gnat cameras, data ferrets, and spy satellites.").

[115] Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, Wired.com (July 18, 2007) available at <http://www.wired.com/politics/law/news/2007/07/fbi_spyware> (last visited Apr 4, 2008).

[116] Application and Affidavit of Norman B. Sanders, Jr., FBI Special Agent, for Search Warrant (filed June 12, 2007), available at <http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf> (last visited Apr 4, 2008).

[117] Id at 3.

already asked its Italian counterparts for help.[118] The FBI had also tracked several leads to several ISPs and had obtained records from those sources, but apparently to no avail.[119]

With no other leads, the FBI used spyware to track the target.[120] Broadly speaking, the term spyware describes programs that run surreptitiously on a computer, tracking users and reporting private information about their computer usage to another person on the Internet.[121] Typically, spyware programs are installed when users are tricked into launching them, sometimes by clicking on a link on a website, opening an emailed attachment, or after being attacked by a network worm or virus.[122]

Historically, spyware programs have been developed in the shadows, funded by small companies, usually seeking to turn the captured usage data into targeted advertising.[123] These companies, which typically call what they sell "adware" not spyware, protest that they are not vandals (unlike most virus writers) but legitimate marketers, unfairly branded as evil or criminal.[124]

The Timberline affidavit reveals that the FBI is now a member of this group of small, ethically-murky developers (or at least purchasers) of spyware. In the affidavit, the agent calls the FBI's tool a Computer & Internet Protocol Address Verifier, or CIPAV.[125] The affidavit goes into very few details, classifying the CIPAV "as a law enforcement sensitive investigative technique, the disclosure of which would likely jeopardize other on-going investigations and/or future use of the technique."[126] In particular, the affidavit makes no mention of how the FBI was planning

---

[118] Id at 11–12.

[119] Id.

[120] Application and Affidavit of Norman B. Sanders, Jr. (cited in note 116).

[121] Alfred Cheng, Comment, *Does Spybot Finally Have Some Allies?: An Analysis of Current Spyware Legislation*, 58 SMU L Rev 1497, 1500–06 (2005) (describing four types of spyware); Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 Berkeley Tech L J 1433, 1434 n 2 (2005) (citing one definition of "spyware" but noting how difficult the term is to define).

[122] See Cheng, 58 SMU L Rev at 1501–04 (cited in note 121) (describing class of spyware that install themselves "without the users' knowledge").

[123] See Ben Edelman, *Why I Can Never Agree with Adware and Spyware*, The Guardian 5 (Jan 25, 2007) ("Adware vendors defend their practices as 'targeted advertising.'").

[124] See Paul Festa, *See You Later, Anti-Gators?*, CNET News.com (Oct 22, 2003), available at <http://www.news.com/See-you-later%2C-anti-Gators/2100-1032_3-5095051.html> (last visited Apr 4, 2008) (describing libel suits brought by Gator against anti-spyware companies stating that "Gator maintains that its software differs from spyware in that people are clearly notified before they download it, and in that they do so in exchange for a service, like the peer-to-peer software.").

[125] Application and Affidavit of Norman B. Sanders, Jr. at 2–3 (cited in note 116).

[126] Id at 5.

to install the CIPAV. The affidavit does reveal that the CIPAV was to collect "the computer's true assigned IP address, MAC address, open communications ports, list of running programs, operating system (type, version, and serial number), Internet browser and version, language encoding, registered computer name, registered company name, current logged-in user name, and Uniform Resource Locator ("URL") that the computer was previously connected to."[127]

The magistrate judge signed the warrant, the CIPAV infected the target's computer, and a suspect was found and arrested.[128] In many ways, this is a great success story. A terrorized community found peace, a terrorist was caught, and the only privacy invaded was the privacy of an alleged criminal. Despite this success, the FBI's use of spyware raises a number of potential troubling harms.

c) Gray-hat harms. The Timberline case shows the great virtue of gray-hat surveillance: it helped the police arrest a terrorist undetectable using traditional methods. But despite this value, the police use of spyware raises great risks.

There are at least five reasons to fear the police acting like hackers and spyware writers. The first is the effect that such behavior will have on the economy and legitimacy of virus and spyware writing. To get into the spyware-authoring game, the police will have two choices, both fraught: develop the software and techniques in-house or contract out to third parties.

The FBI's 2008 budget request allocates $220,000 to "purchase highly specialized equipment and technical tools used for covert/overt search and seizure forensic operations .... This funding will allow the technology challenges including bypass, defeat, or compromise of computer systems."[129] This is a relatively miniscule line item in the FBI's six billion dollar annual budget,[130] but in a world where criminals use more and better privacy-enhancing technology, this line item will likely grow in absolute dollars and as a percentage of the entire FBI budget. This would be money poured into the development of tools that in the wrong hands could be used for very bad purposes; it would be

---

[127] Id.

[128] Poulsen, *FBI's Secret Spyware* (cited in note 115).

[129] Federal Bureau of Investigation, *FY 2008 Authorization and Budget Request to Congress* 4-69 to 4-70 (2008), available at <http://www.usdoj.gov/jmd/2008justification/office/33_01_justification.doc> (last visited Apr 4, 2008).

[130] Id.

money expended by the government to advance the state of a not-so-noble art.

It would be naïve to hope that the FBI would take information from the gray-hat community without giving back in kind. For one thing these tools would be distributed, sometimes to other law enforcement agencies and more troublingly through installation on targets' computers. In the Timberline case, the target's computer was infected by the FBI's program, and even the FBI probably has no way of knowing whether copies still reside in other computers or email inboxes. If the FBI were to advance significantly the art of computer exploitation—for example, if it were to discover an undocumented OS vulnerability[131]—it would need to unleash its innovation "in the wild" in order to gain its benefits, giving others the chance to find and reverse engineer the code.[132]

Worse than in-house development is providing government money to third parties to develop these tools, thereby placing an FBI seal of approval on these activities, legitimizing and buttressing a previously underground, shadowy market in exploits and vulnerabilities.[133]

Second, these acts violate user privacy. Unlike many police practices, such as snitches or pen registers, which target the unwisely trustworthy,[134] spyware tends to target people who have intentionally sought privacy through encryption or other means. This is, in part, why many laws have been enacted targeting spyware, hacking, and viruses as criminal privacy violations.[135]

---

[131] Software security flaws that are unknown until they are first launched are known as "zero day" vulnerabilities. See generally Kevin D. Mitnick and William L. Simon, *The Art of Intrusion* (Wiley 2005).

[132] See Gregg Keizer, *What We Know (Now) About the FBI's CIPAV Spyware*, Computerworld (July 31, 2007) (speculating that the spyware used by FBI in the Timberline High case exploited a known, not zero day, vulnerability).

[133] Some scholars argue that a market for vulnerabilities would lead to better security. See, for example, Rainer Böhme, *Vulnerability Markets: What Is the Economic Value of a Zero-Day Exploit?*, Private Investigations (Proc of 22nd Chaos Communication Congress), available at <http://www.inf.tu-dresden.de/~rb21/publications/Boehme2005_22C3_VulnerabilityMarkets.pdf> (last visited Apr 4, 2008); Micah Schwalb, *Exploit Derivatives and National Security*, 9 Yale J L & Tech 162 (2007).

[134] *Hoffa v United States*, 385 US 293, 302 (1966) (holding use of informant to obtain incriminating statements not a Fourth Amendment search or seizure); *Smith v Maryland*, 442 US 735 (1979) (holding use of pen register not a Fourth Amendment search).

[135] Many states have passed laws attempting to provide criminal and civil liability against people who create and distribute some forms of spyware. See Peter Brown, *Spyware and Pretexting: Recent Developments*, 894 PLI/Pat 267, 273 n 7 (2007) (listing state statutes). The Federal government has proposed similar laws but has not passed any to date. Id at 274 & n 12. Hacking and viruses are prohibited under various Federal laws. See, for example, Violent Crime Control and Law Enforcement Act of 1994, 18 USC

Of course, this is a variation on an old theme. The police have long violated criminal laws and social norms to accomplish their goals.[136] But this history is neither worth celebrating nor perpetuating. Ironically, by deploying better privacy-enhancing technology users may be exposing themselves to new kinds of governmental privacy invasions.[137]

Third, the government's use of spyware, hacking, and viruses to search and seize would raise many tricky, novel Fourth Amendment questions.[138] These difficult questions would pose a risk of muddying even more the already-confusing body of Fourth Amendment law.

Fourth, there is a significant accountability problem. For one thing, the police would be able to send spyware and viruses directly, without involving third party intermediaries like ISPs, placing more of their activities in the shadows and making the

---

§ 1030 (2000 & Supp 2005) (banning various forms of computer hacking); Communications Assistance for Law Enforcement Act, 18 USC § 2511 (2000 & Supp 2005) (prohibiting wiretapping, including the interception of electronic communications); Electronic Communications Privacy Act of 1986, codified within various sections of title 18 at § 2701 (2000 & Supp 2005) (prohibiting access to communications stored on an ISP's servers); Id at § 3121 (prohibiting the use of pen registers and trap and trace devices, defined elsewhere as devices configured to capture "dialing, routing, addressing and signaling information"). Some of these laws have express exceptions for law enforcement investigations. See, for example, 18 USC § 1030(f) ("This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.").

136 See, for example, *Olmstead v United States*, 277 US 438, 480 (1928) (Brandeis dissenting) ("To prove its case, the government was obliged to lay bare the crimes committed by its officers on its behalf. A federal court should not permit such a prosecution to continue.").

137 Others have made similar arguments:

> *Encryption, oddly enough, may lead to greater violations of privacy than would otherwise have occurred.* For example, if investigators encounter unbreakable encryption on a wiretap, they may well pursue other methods of surveillance, including hidden microphones, cameras, and other sensors installed on the subject's premises. Undercover operations are another alternative. These methods—which are quite legal under certain conditions—are often not only more dangerous to the subject and to law enforcement officials, but also more invasive to the subject's privacy.

Amitai Etzioni, *The Limits of Privacy*, 80 (Basic 1999).

138 See, for example, *United States v Forrester*, 495 F3d 1041 (9th Cir 2007) (holding that the ISP-assisted monitoring by the government of the to/from lines of e-mail messages, the IP addresses of websites visited, and the total volume of information sent did not violate the Fourth Amendment); *United States v Gorshkov*, No CR00-550C, 2001 WL 1024026, at *1 (W D Wash 2001) (analyzing whether FBI agents violated the Fourth Amendment when they accessed and copied files located in Russia of a Russian citizen under surveillance in the U.S.)

acts less likely to come to public attention.[139] Even worse, these tools would be so complex and sophisticated that it is likely that only the programmers developing them would be well positioned to compare risks and benefits. Very likely, not even the line agents they work with nor their superiors would understand the tools as well as they should. The problem would get worse up the chain of authority, with the supposedly most politically accountable people of all—appointed officials in the front offices of the FBI and DOJ—understanding the tools only through many layers of translation, analogy, and metaphor.

Finally, we should be concerned about bugs. Software fails at predictable rates.[140] Software developed to solve a one-off problem is more susceptible to bugs than software developed for a long-term problem. Bugs can reveal more private information than intended or allowed; they can cause damage to computers and networks; and they can run out of control.

3. Government countermeasures III: indiscriminate surveillance.

The other likely response is more indiscriminate surveillance. Deafened by encryption, the police might argue for more dragnet surveillance, engaging in massive wiretapping or data mining. They will argue that although they cannot listen in on the conversations of their targets, they can still gather evidence by looking for patterns of behavior and by reconstructing networks of relationships.[141]

---

[139] Consider how long it took for the public to learn about the NSA's surveillance of online communications, and financial transactions despite the involvement of dozens, if not hundreds, of employees of third-party intermediaries. See James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, NY Times A1 (Dec 16, 2005) (reporting about presidential order first signed in 2002); Eric Lichtblau and James Risen, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, NY Times A1 (June 23, 2006) (reporting on program initiated shortly after September 1, 2001); Mark Klein, *Wiretap Whistle-Blower's Account*, Wired.com (April 7, 2006), available at <http://www.wired.com/science/discoveries/news/2006/04/70621> (last visited Apr 4, 2008) (public statement of former AT&T technician Mark Klein, who revealed details of AT&T's participation in NSA wiretapping).

[140] See Ohm, 41 UC Davis L Rev at 1371 n 234 (cited in note 91).

[141] See generally, David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 Yale L J 628, 630 (2005) ("The 'mosaic theory' describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information.").

D. Beyond the Thought Experiment

Because privacy-enhancing technology is created through an arms race, perfection will probably never be achieved.[142] Every advance in privacy enhancement will be met by an advance in transparency forcing. Given this fact, this discussion has been at best a thought experiment, an attempt to examine the harms that would occur if we were ever to have perfect technology.

The lessons of the thought experiment should inform the debate on two levels. First, it might give advocates who desire perfection a moment's pause.[143] Staunch advocates will continue to press for perfection, of course, but they should be cautioned to be careful what they wish for. For example, EFF could continue to support projects like TOR in ways that make the software more robust and capable, but EFF should not encourage operating system manufacturers to incorporate TOR-like technology onto every desktop.

Second, for non-advocates, and especially for the technologists and policymakers who will shape the next generation of privacy- and transparency-enhancing technology, a better appreciation of the limits of perfection could help guide future decision-making. Software developers should consider the dangers of perfection when planning how to invest time and resources in improving privacy technology. The next time policymakers are asked to consider a bill like CALEA, they should first assess whether technology is closing in on perfection. Even if it is, they should craft laws and regulations that do not try to shift technology all the way from perfect privacy to perfect transparency, as CALEA tries to do, but they should instead focus on making technology "less perfect."[144]

The problem with acting on this advice, however, is it relies on the ability to assess when a technology is "perfect" or "near perfect" in providing privacy and transparency. Thus far, this Article has only sketched what is meant by these muddy terms. The next Part seeks to provide a more nuanced, less monolithic understanding of technological capability, and a tool for mapping technologies across the capability landscape. In particular, mov-

---

[142] See Part I B; Brin, *The Transparent Society* at 184 (cited in note 8) ("Millions of expert-worker-hours have already gone into perfecting the encryption-anonymity option, without coming anywhere near perfection so far.").

[143] Part I C.

[144] See Part IV B.

ing away from perfection encourages greater attention to struggle. How can struggle be introduced and maintained?

III. MEASURING PERFECTION

If we are convinced that both perfect privacy and perfect transparency are undesirable and should be avoided, we need a metric for measuring the state of technology at a given time. Is a privacy-enhancing technology too effective? Are there too many transparency-enhancing tools? Again, the common metric for this kind of measurement is the spectrum from no privacy to no transparency, but as we shall see, this model is of little use to policymakers. Before looking at the spectrum model's shortcomings, consider a few observations about the causes of our inclination to perfection.

A. The Source of the Misguided Calls for Perfection

Calls for technological perfection stem from many aspects of the debate between privacy and transparency. Legal scholars frame privacy's and transparency's harms in all-or-nothing ways, thereby contributing directly to mistaken calls for perfection. Computer scientists do something very similar. Advocates rely too much on idealized standard bearers—terrorists and freedom fighters—without recognizing that technology cannot discriminate between the two groups.

1. Perfection and the connection to scholarship.

Scholars who write about information privacy conceive of the topic in a manner that leads to calls for perfection. They imagine that the harms from transparency and privacy are catastrophic and accrue at the slightest breach. With one revelation or misuse of personal information, people's lives unravel.

Consider first how scholars talk about harms from privacy invasions to a victim's sense of repose. The sense of repose is treated like a delicate, fragile thing. It shatters as soon as an individual senses any fear of being watched. Meanwhile, scholars who urge transparency take a similar, one-misstep-and-disaster approach when arguing for broad law enforcement authorities.[145]

---

[145] See Etzioni, *The Limits of Privacy* at 81 (cited in note 137) ("Consideration should be given, however, not only to the probability that a given event will occur but also the magnitude of the disaster if it does.").

Instead of thinking of transparency's harms as all-or-nothing, maybe it is more accurate to think of an almost-mathematical relationship between transparency (or privacy) and harm. If one pair of conspiratorial criminals could communicate without the FBI listening in, there would be much less to worry about than if one hundred or one thousand could do the same. Likewise, if Congress could raise struggle and decrease the number of tools of perfect privacy the FBI should welcome the change even if other perfect privacy tools remain.

This works for privacy-enhancing tools as well; if policy changes could empower five more dissidents to communicate in private, that would be cause for celebration, even if five hundred still could not. By focusing on struggle, we can learn to celebrate and strive for incremental results, rather than lament our inability to get perfection or to find balance.

2. Perfection and computer science.

Computer scientists view the world of technological privacy in a similarly binary way. They import this from the way they think about and research cryptography. Cryptographers measure their algorithms against the ideal of perfection, seeing anything short of perfection as flawed and therefore non-robust. Cryptographic methods are measured by the number of years it would take for a brute-force attacker to crack the scheme.[146] An encryption protocol that theoretically would require three trillion years to crack using brute force methods would be considered broken and in need of replacement if a vulnerability would allow a crack that takes merely one trillion years.[147] To the lay observer, this may seem wildly overcautious, but it is actually pragmatic, because experience has shown that any theoretical flaw, even one

---

[146] See Schneier, *Applied Cryptography* at 153 (cited in note 37) (displaying table of "Average Time Estimates for a Hardware Brute-Force Attack in 1995").

[147] As an example of both of these fears about "broken" algorithms, consider the MD5 hash algorithm. In 1996, MD5 was claimed to be vulnerable because its signature-making feature could be faked in less than brute force time. Hans Dobbertin, *Cryptanalysis of MD5* Compress (1996), available at <http://citeseer.ist.psu.edu/68442.html> (last visited Apr 4, 2008). To the lay observer, this probably would not have seemed to be an important moment, because breaking the algorithm meant spending many times the age of the universe. But the research led in 2004 to many practical implementations of faked MD5 signatures, computed relatively rapidly. Xiaoyun Wang and Hongbo Yu, *How to Break MD5 and Other Hash Functions*, in Ronald Cramer, ed, *Advances in Cryptology—Eurocrypt 2005*, 23 (Springer Berlin 2005). In other words, the early, theoretical fears of broken MD5 led down the road to realistic attacks.

that requires geologic time to exploit, will lead eventually to exploits that operate on a human timescale.[148]

But this tendency to see encryption only as "perfect or flawed" translates poorly into the world of privacy policy. Cryptographers, who are sometimes asked to advise on the concept of "privacy," may confuse theory and policy. That millions of users continue to use a flawed wireless encryption algorithm may seem outrageous from a theoretical, technical point of view, but from a policy or economic point of view, it may be perfectly reasonable.

3. The freedom fighter/criminal equivalence.

Turn next to advocates. Each side in the debate over privacy or transparency has embraced a standard bearer, the object of its hopes or fears. For those who urge privacy, he is the heroic freedom fighter, the dissident living under a totalitarian regime.[149] For those who urge transparency, he is the villainous criminal or terrorist.

Technology cannot distinguish between saint and sinner. Although it is nice to imagine that dissidents can access technology that criminals cannot, this is an impossible hope.[150] Technology, once released, is available to all.

In fact, the forces that distribute technology unequally across a population probably behave the opposite of what we would choose. These forces seem likely to deprive dissidents of tools that criminals will have, not the other way around. For ex-

---

[148] See Wang and Yu, "How to Break MD5 and Other Hash Functions," (cited in note 150) (describing vulnerability in prominent "digesting" algorithm MD5 which can be exploited in "15 minutes up to an hour computation time").

[149] See notes 184–85 and accompanying text (describing the work of Patrick Ball to teach dissidents about technologies of privacy).

[150] As Stewart Baker—then General Counsel for the NSA—put it during the Clipper Chip debate:

> Take for example the campaign to distribute PGP . . . encryption on the Internet. Some argue that widespread availability of this encryption will help Latvian freedom fighters today and American freedom fighters tomorrow. Well, not quite. Rather, one of the earliest users of PGP was a high-tech pedophile in Santa Clara, California. He used PGP to encrypt files that, police suspect, include a diary of his contacts with susceptible young boys using computer bulletin boards all over the country. . . . If unescrowed encryption becomes ubiquitous, there will be many more stories like this. We can't afford as a society to protect pedophiles and criminals today just to keep alive the far-fetched notion that some future tyrant will be brought down by guerrillas wearing bandoleers and pocket protectors and sending PGP-encrypted messages to each other across cyberspace.

Stewart A. Baker, *Don't Worry Be Happy*, Wired 2.06 (June 1994).

ample, people often need resources—money, skill, training, experience—to use tools. Although there are both well-funded criminals and well-supported freedom fighters, one suspects that the wealthiest criminals command more resources than the best-supported dissidents. If this were true and if a new law or regulation would mean that technology would be limited only to those with resources,[151] then sadly, dissidents would lose access long before criminals do.

B. Critiquing the One-Dimensional Model

Thus far, technology has been viewed one dimensionally, from providing more transparency to more privacy. The metaphor has been a spectrum, and policymakers have been depicted as selecting an optimal place along that spectrum. The spectrum is a problematic metaphor.

To understand why, ask, how does the spectrum encourage people to value or measure the relative privacy provided by a tool? What does it mean to say that TOR provides "better" or "more" privacy than BitTorrent? Most likely, assertions like this refer to a quality of software that could be called robustness. To be robust, a cryptographic tool must be built upon fundamental, mathematical algorithmic underpinnings that are theoretically sound. But this is not enough, as the best theory is useless unless software developers created a tool that correctly implements the theory.

When a technology is said to provide "good privacy," the speaker usually means nothing more but that the tool is robust. This is an incomplete assessment of privacy because it neglects the many other factors that make a tool privacy-enhancing. By viewing technological privacy as a one-dimensional spectrum, a volume knob, a fuel gauge, technologists and policymakers are neglecting these other factors.

Further, as discussed earlier,[152] while a drive toward perfection is appropriate for scientists designing cryptographic protocols, it does not translate well into policy. Policymakers and advocates, perhaps influenced by such computer scientists, come to believe that the only choices are perfect privacy or perfect trans-

---

[151] See John Markoff, *Technology: Wrestling Over the Key to the Codes*, NY Times 9 (May 9, 1993) (quoting Whitfield Diffie: "By codifying the Government's power to spy invisibly on these contacts, we take a giant step toward a world in which privacy belongs only to the wealthy, the powerful and, perhaps, the criminals.").

[152] See Part III A 2.

parency. The participants in the debate, with the spectrum metaphor in mind, are likely to see technology problems as either-or questions. Should we have absolute privacy or none?

Consider again the CALEA debate. CALEA is an either-or solution. In place of wiretap-proof communications technologies, which are bad, Congress and the FCC force wiretap-enabling backdoors, which are good. Framing the problem and the solution like this flows directly from the metaphor. Swing the pendulum, push the slider, flick the switch, from one pole to the other.

A final problem with one dimensionality is that it too often fosters slippery slope arguments. The surface of a slippery slope, after all, is a one-dimensional path from point A to point B. When privacy and transparency are pictured as a single, measurable quantity like robustness, it is easy for advocates to fix on the endpoint in the direction they want to move. Further, it becomes easy to demonize the endpoint at the opposite end of the spectrum, because that way lies danger. Technologically-provided privacy and transparency should instead be seen as values that map across several dimensions, with slopes in many directions, some going up, others going down, with lots of plateaus in between, across a bumpy landscape. Instead of an inexorable drive toward slippery slope arguments, multi-dimensional thinking could lead toward intermediate plateaus, to spaces of good enough privacy, to more nuanced positions.

C. Adding a Second Dimension: The Privacy Matrix

All of these problems diminish when other values or attributes are considered. Policymakers and technologists should consider a complex of different things that add up to a given level of privacy or transparency. But what else besides a tool's robustness should be considered? If one dimension would be too few, how many dimensions should be considered? Two? Three? More?

The answer is to focus on the harms described in Part II. If these were the most important problems with perfection, then varying the level of privacy would mean varying things that contribute to these harms. What features of software cause the type of harms described?

The other touchstone for developing the model is simplicity. What is sought is a tool that regulators and innovators can use to measure the state of technology and map it onto policy concerns.

In the end, only one other value—albeit a compound value made up of separate constituent values—is important enough and maps closely enough onto Part II's harms to be included in

the analysis, especially given the goal of simplicity: a measure of a tool's cost.

One quick note—the discussion that follows will focus entirely on privacy-enhancing technology, without stepping through the complementary discussion about transparency-enhancing technology. This is to simplify the discussion. Everything said in what follows can be restated as a mirror-image about transparency.

Why should policymakers focus only on robustness and cost, excluding other considerations? Let us look at each in turn.

1. Robustness.

Although there are pitfalls to a single-minded focus on a tool's robustness at the expense of every other attribute, it remains one of the most relevant measures of technology. The robustness of a tool is the amount of effort required by an adversary to defeat the privacy provided.

Robustness almost always refers to the strength of the cryptography underlying the privacy technology. The robustness of cryptography turns on a few factors including the cryptographic method chosen (the algorithm), the success of the specific software implementation (are there bugs?) and, most famously, the length of the key used to encrypt. Holding the first two factors constant, the longer the key used, the harder it is for would-be codebreakers to decipher the encoded message. Applying the three factors to an example, communications can be encrypted using the Triple-DES algorithm, as implemented by the OpenSSH open source programming team, with 64-bit keys.[153] With the same algorithm and implementation, 128-bit keys would provide more robustness.

It is crucial to remember also that technologically robust privacy is possible without encryption. For example, many WiFi hotspots tend to be unencrypted, yet they still provide a good level of anonymity because they allow people to walk up, connect, communicate, and leave. If the communication sent during that brief association were one that someone would like to track—a death threat or a call to overthrow a ruthless dictator, for example—the user's identity would probably be hard to find.

---

[153] See Neils Ferguson and Bruce Schneier, *Practical Cryptography* (Wiley 2003) (describing OpenSSH).

2. Cost.

The other value that is as important as robustness to measuring the privacy of a tool or groups of tools is a group of attributes collectively referred to as "cost." Technologies are installed and used only if users are willing and able to meet their costs. A robust but high-cost technology will be used only by some people, even if others could benefit from its robustness. Conversely, a non-robust but low-cost technology may be used by many people, without providing a significant amount of privacy.

Cost refers to a number of different things. Perhaps the most important component of cost is a tool's *ease-of-use*. The most robust privacy-enhancing technology would be worthless if it were so difficult to use that nobody ever uses it.[154] Ease-of-use is often a measure of user-friendliness. Operating systems with graphical user interfaces are much easier to use—they are more user-friendly—than the command-line interfaces that came before.[155] Similarly, tools used to encrypt email messages have historically been very hard to use.[156] At one point, sending an encrypted email message—a message that only a person with a previously-agreed-upon key could read—required installing a piece of dedicated software, authoring the email message in an email program, cutting-and-pasting that message into the encryption software, clicking a button, cutting-and-pasting the resulting ciphertext back into the email program, and, finally, sending.[157] Even this long list neglects the separate, equally complex prerequisite task of trading secret keys.

Another type of user cost is *accessibility*, which encompasses two separate attributes—ease of installation and default settings. As for the first, technology is most easy to install—in that it need not be installed—if it comes bundled with a computer.[158] It is less easy to install if it needs to be downloaded from the

---

[154] See Diffie and Landau, *Privacy on the Line* at 206 (cited in note 3) ("In writing PGP, Phil Zimmermann did something for cryptography that no technical paper could do: he gave people who were concerned with privacy but were not cryptographers (and not necessarily even programmers) a tool they could use to protect their communications.").

[155] Consider Neal Stephenson, *In the Beginning . . . Was the Command Line* (Perennial 1999).

[156] See Simson L. Garfinkel, *Thesis: Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable* Ch 5 (MIT 2005); Whitten and Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* (cited in note 15).

[157] Garfinkel, *Design Principles and Patterns for Computer Systems* at Ch 5 (cited in note 156).

[158] J. Gregory Sidak, *An Antitrust Rule for Software Integration*, 18 Yale J Reg 1 (2001) (describing the practice of software bundling).

Internet. The hardest technologies to install are those that require extensive configuration or source code compilation.

There is an extensive literature about the crucial role of default choices in law.[159] More recently, scholars have applied this earlier work to discuss how software defaults can have a profound impact on online conflict and regulatory decisions.[160]

Cost is too often ignored in debates about technological privacy. An obsessive focus on whether the NSA can break a particular tool often masks the much more important question—is a tool likely to end up in the hands of people needing privacy, or will the tool's costs limit it to the computers of a very few?

3. The privacy matrix.

These two dimensions—robustness and cost—can be mapped on a two-by-two matrix, with the rows representing cost and the columns representing robustness.

FIGURE 1

Cost / Privacy	Not Robust	Robust
Hard to Use / Hard to Get / Banned	I First generation wireless privacy (WEP)	II Anonymizers (TOR), older encryption tools for stored files (PGP), older encrypted tunnel tools (SSL)
Easy to Use / Easy to Get / Installed by Default	III IP addresses, Gmail	IV Newer encrypted tunnel tools (Skype and BitTorrent), newer encryption tools for stored files (BitLocker and EFS))

[159] See, for example, Ian Ayres and Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale L J 87 (1989).

[160] See, for example, Jay P. Kesan and Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 Notre Dame L Rev 583 (2006); Kang, 50 Stan L Rev at 1246–65 (cited in note 88) (considering default rules for online information privacy analyses).

It is hoped that Figure 1 becomes a standard tool for measuring the impact and regulation of privacy-impacting software. We can map various technologies into the four quadrants of the matrix. *Type I* technologies are hard to use and provide some, but not very robust, privacy. *Type II* technologies provide robust levels of privacy but are difficult to use or install. A large assortment of present-day technology falls in this category. *Type III* technologies are very easy to use and install, often because they come built-in with a computer or because they can be downloaded directly and easily from the Internet, but they do not provide a robust level of privacy. Finally, *Type IV* tools provide very good privacy and are easy to use and install. Although historically there have not been many products that fit within Type IV, the number is increasing.

To better understand the differences and connections between the four quadrants of the matrix, consider the following examples, grouped into the familiar three categories of privacy bestowed: tunnel, stored, and identity privacy.

4. Examples: mapping tunnel privacy.

The typical tunnel privacy problem is this: Alice would like to use the Internet to chat with Bob, but she is worried about the wiretapping Eves of the world.

If Alice and Bob choose not to use any privacy-enhancing technology, then by default they would be choosing a Type III—low cost, low robustness—solution. In fact, there is almost no cost in this choice: the tools they need to communicate via email or instant messaging are installed on their computers by default. These are consumer-grade programs designed for average users, meaning the software is probably very easy to use. Still, Alice and Bob would be almost unprotected from wiretappers when using Type III solutions.[161]

When Alice moves her laptop onto a wireless, WiFi network, she may (or may not) have the opportunity for a bit more tunnel privacy. An infamous Type I—high cost, low robustness—form of tunnel privacy technology is Wireless Equivalent Privacy ("WEP") which is used to protect communications being sent

[161] "Almost unprotected," not "completely unprotected" because the Internet itself provides some latent privacy protection. Just as a would-be land-line phone wiretapper needs to find a wire across which a particular conversation flows, on the Internet, a would-be wiretapper needs access to a communications hub across which a particular e-mail or chat session routes.

across WiFi networks. WEP is infamous because it is known to be flawed. Soon after WEP was released, cryptanalysts discovered weaknesses in WEP's encryption.[162] A motivated third party could intercept encrypted WEP content and decipher the communications. As if this were not enough, WEP networks are also difficult to configure, requiring a user to key-in ten or twenty-six seemingly random characters.

WEP spotlights a puzzle about Type I technology: why does the market give rise to and support the growth of Type I technologies? Should not a well-functioning market preclude or kill off Type I technologies, as consumers opt for cheaper or easier-to-use alternatives?[163]

In fact, the market has already provided an alternative to WEP. The Wi-Fi Alliance, an industry trade group, created a successor system known as Wi-Fi Protected Access ("WPA"). WPA is more robust than WEP, making it perhaps Type II technology, and it is also a bit easier to use, particularly because it allows a server to have one, user-selected password, which can be entered in a way that is likely familiar to users.[164]

The story of the slow transition from WEP to WPA demonstrates why markets sometimes create Type I technologies. Especially when privacy is not a top priority for a software developer, or when the developer does not have access to well-trained cryptographers, attempts to engineer privacy will fall flat.[165] The

---

[162] See Nancy Cam-Winget, et al, *Security Flaws in 802.11 Data Link Protocols*, 46 Commun of the Assoc for Computing Machinery 35 (May 2003) ("The . . . attack is devastating to WEP. Once the WEP key is discovered, all security is lost.").

[163] One explanation for the presence of Type I encryption technology is the government's regulation of the export of cryptography. Froomkin, 1996 U Chi Legal F 19 (cited in note 5) ("Largely because of the ban on export of strong cryptography, there is today no strong mass-market standard cryptographic product within the U.S. even though a considerable mathematical and programming base is fully capable of creating one."). After the vulnerabilities in WEP were revealed, the Chair of the standards body responsible for WEP blamed, among many other things, the government's export controls. See *Chair of IEEE 802.11 Responds to WEP Security Flaws*, Slashdot.org, Feb. 15, 2001 available at <http://it.slashdot.org/article.pl?sid=01/02/15/1745204> (quoting Stuart J. Kerry, Chair of IEEE 802.11 Standards Working Group: "In addition it needs to be noted that the choice of encryption algorithms by IEEE 802.11 are not purely technical decisions but they are limited by government export law restrictions as well.") (last visited Apr 4, 2008).

[164] Although WPA is easier to use than WEP, it probably is not easy enough to use to classify it as Type IV.

[165] Comparing these Type I and Type III examples demonstrates a limitation of the two-by-two matrix: it masks some relatively fine distinctions. For example, although they are both in the same robustness column, Type I technologies often provide better privacy protection than Type III technologies. This is because Type III technologies—easy-to-use but non-robust—include the many default situations in which user privacy is unprotected. Better than a two-by-two matrix, perhaps, is a scatter plot across X- and Y-axes.

market seems slow to correct these Type I "mistakes." According to many studies, years after WEP's vulnerabilities were disclosed and WPA was offered as an alternative, WEP is still widely deployed.[166]

For Type II—high cost, high robustness—tunnel privacy, Alice and Bob can turn to encrypted tunnels. With a lot of technological know-how, the pair can establish a dedicated encrypted channel—a form of the Virtual Private Network, or VPN, often used by business travelers—through which they could stuff email or instant messages.[167]

Skype is a classic example of Type IV tunnel privacy.[168] Although some expertise is needed before a user can find, download, and install Skype, this process has been made relatively easy to do, and once the software is installed, users enjoy the benefits of encrypted communication, whether they know they have it or not. All of the difficulty Alice and Bob encountered in configuring a VPN would be handled by Skype's programmers, who would have hidden all of the technical detail beneath Skype's friendly user interface.

Some of the costless, privacy-less Type III technologies exist further to the left along the X-axis than many Type I offerings.

[166] Peter Sayer, *Don't Use WEP, Say German Security Researchers*, InfoWorld.com (April 4, 2007), available at <http://www.infoworld.com/article/07/04/04/HNdontusewep_1.html> (last visited Apr 4, 2008) ("Many networks still rely on WEP for security: 59 percent of the 15,000 Wi-Fi networks surveyed in a large German city in September 2006 used it, with only 18 percent using the newer WPA (Wi-Fi Protected Access) protocol to encrypt traffic. A survey of 490 networks in a smaller German city last month found 46 percent still using WEP, and 27 percent using WPA.").

[167] In fact, there is a user-friendlier form of encrypted tunnel that even casual web browsers tend to know about known as SSL or Secure Sockets Layer. SSL is familiar, if not by name then by the little "lock" icon that sometimes appears in a web browser. When the little lock appears, web pages are wrapped in a tunnel of encryption as they are downloaded. To use SSL, all a web surfer needs to do is visit a website hosted by a provider who provides SSL.

Is SSL a Type IV—low cost, high robustness—technology? After all, any user with virtually any web browser can use SSL with ease, just by entering a URL or clicking on a link. SSL seems as low-cost as a technology can be. On the contrary, although SSL puts very few burdens on the user, it is still difficult for the person (or institution) communicating on the other end—the person setting up the SSL-protected web page. If Alice wants Bob to be able to download secret launch codes on an SSL-protected website, Alice needs to enable SSL on her web server, meaning at the very least she needs to juggle secret keys. Furthermore, SSL adds cryptographic overhead to a web transfer, slowing it down. Because of these costs, webmasters tend to use SSL only when it is important, and there are many more unencrypted than encrypted web pages on the web.

[168] *Staying Safe on Skype: Privacy FAQs*, available at <http://www.skype.com/security/safety/safety.html> (last visited May 6, 2008) ("When you call another Skype user your call is encrypted with strong encryption algorithms ensuring you privacy.").

5. Examples: mapping identity privacy.

Consider a few examples of technologies which provide identity privacy. Perhaps the most widely-used example of Type III identity privacy is the privacy afforded by pseudonymous free email account services like Yahoo! Mail, Microsoft's Hotmail, and Google's Gmail. With services such as these, users can set up a new email account in minutes. Although messages sent with such an account are protected by a pretty good level of pseudonymity which the average user might view as very robust, the privacy protection has limits.

First, to every outbound email message sent from Hotmail, the service appends metadata called the X-Originating-IP header.[169] This short string of data reveals to the recipient of the message (and anybody in between who happens to be listening) the IP address of the computer from which the message was sent. Second, all of these services retain records relating to users and messages found on its servers. Law enforcement agents armed with appropriate legal process can compel these services to reveal that information.

An example of Type II identity privacy software is TOR, or The Onion Router.[170] TOR is a type of "mix network."[171] A mix network is structured in some ways like a peer-to-peer software trading network. It lets people send Internet communications through a random series of peer computers also running TOR before arriving at its destination. Through a series of clever cryptographic tricks (beyond the scope of this Article), none of the computers in the middle of the path can access the content of the communications nor discover the IP addresses of *both* the sending and receiving computers.[172] Despite its promise, TOR does not come pre-installed on any operating system, and although TOR is easier to use than the consumer encryption available a decade ago,[173] it is still a challenge.[174]

---

169 See Casey, *Digital Evidence and Computer Crime* at 507 (cited in note 41). Yahoo! and Gmail provide the same information, in different e-mail headers.

170 <http://torproject.org> (last visited Apr 4, 2008).

171 See David L. Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, 24 Commun of the Assoc for Computing Machinery 84 (Feb 1981) (seminal paper on mix networks).

172 The first computer in the chain knows the IP address of the sending computer but not the receiving computer. The last computer contacted knows the IP address of the receiving computer but not the sending computer.

173 See Whitten and Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* (cited in note 15).

6. Examples: mapping endpoint privacy.

Finally, focus on some endpoint privacy tools. At least historically, most endpoint privacy has come from Type II encryption tools that are robust but difficult for the average user to use. For many years Pretty Good Privacy ("PGP") by Phil Zimmerman was hailed as an easy-to-use and robust program which could encrypt, among other things, the content of stored email messages. The reality failed to meet the hype. First, users had to download and install PGP, no doubt made more difficult because the U.S. government suggested that PGP could not be downloaded over the Internet without violating laws and regulations limiting the export of cryptography.[175] Visitors to the PGP website had to choose between U.S. based and foreign-based servers, with ominous-sounding warnings about the legal consequences of an incorrect choice. Once a user managed to install PGP, she would then be faced with the intricacies of key management, a notoriously tricky problem raised by all public key cryptography solutions.[176] Users in the mid-1990s were forced to save keys to floppy disk or on printouts, and they were exhorted not to lose those critical physical objects, lest they lose access to all of their secrets.

With time, some endpoint privacy tools have become much easier to use, perhaps crossing the border between Types II and IV. An example of Type IV endpoint privacy is Microsoft's BitLocker and EFS system. This operating system feature encrypts all data on a user's computer's hard drive. While the user is logged in, the data is decrypted in the background and on the fly, appearing to the user as ordinary data. But when the computer is shut down, the data sits on the computer's hard drive protected by encryption, and even the FBI would find it difficult if not impossible to decrypt the information.[177] Both BitLocker

---

[174] For example, a researcher with the Berkman Center posted what he hoped was a "simpler, more step by step guide" to using TOR for bloggers which—in Step One alone—required downloading and installing four separate pieces of software. Ethan Zuckerman, *Anonymous Blogging with TOR*, Global Voices Blog, available at <http://www.globalvoicesonline.org/advocacy/anonymous-blogging-with-tor/> (last visited Apr 4, 2008).

[175] Consider Matthew Parker Voors, *Encryption Regulation in the Wake of September 11, 2001: Must We Protect National Security at the Expense of the Economy?*, 55 Fed Commun L J 331 (2003).

[176] See Ferguson and Schneier, *Practical Cryptography* at 309 (cited in note 153) (calling key management "without a doubt, the most difficult issue in cryptographic systems").

[177] A person with physical access to a BitLocker/EFS-protected computer may be able to read the key out of memory. See John Markoff, *Researchers Find Way to Steal En-*

and EFS come installed with some versions of Windows Vista.[178] Perhaps in an acknowledgement of law enforcement concerns, BitLocker is never enabled by default.[179]

IV. STRUGGLE

The discussion has thus far has been largely descriptive. The two-dimensional view of technological privacy and transparency, the mapping of this into four general quadrants of technology, and the identification of the harms that inhere with each type, can be used to create a sort of "report card" of the state of any particular technology. It can be used solely as a descriptive tool to passively track the twists and turns of future technological development, enabling better informed policy discussions.

I also advance a prescriptive and normative goal: to use the taxonomy, incorporating the earlier discussion of struggle, to argue for a particular level and type of technologically-provided privacy and transparency.

The first task will be to map the various harms described in Part II onto the various quadrants of the matrix. Second, the focus will shift to a much more dynamic analysis of the matrix, spending more time than allotted during the descriptive phase on pairwise comparisons between the quadrants. We know for example, that the FBI hopes for non-robust privacy protection (Types I and III) and that privacy advocates hope for robust technology (Types II and IV); this is the traditional divide, the one presented by those who see the world as a spectrum, and the one that I have claimed has led to intractable debates and has paralyzed policymakers. The great value of the matrix's added dimension is to broaden from a single-minded focus on robustness and to force people to make comparisons, for example, between the rows and the corners of the model. For example, as

---

crypted Data, NY Times C1 (Feb 22, 2008); J. Alex Halderman, et al, *Lest We Remember: Cold Boot Attacks on Encryption Keys*, Draft Paper of the Center for Information Technology Policy at Princeton University, available at <http://citp.princeton.edu/memory/> (last visited Apr 4, 2008).

[178] Morris, *Notes on Vista Forensics* cited in note 76) (reporting that BitLocker is available in Vista Enterprise and Ultimate and EFS is available in the Business, Enterprise, and Ultimate editions).

[179] Id ("Initially there were some concerns within the computer forensics community that the proposed encryption features of Vista, especially BitLocker, would result in a huge increase in the amount of encrypted data confronting examiners. However, it is now clear that these features will be limited to the higher end editions of Vista only and are not implemented by default."). EFS is also not enabled by default, but it "simply requires a checkbox to be ticked in the file or folder's properties to be enabled." Id.

between different non-robust tools, would the FBI prefer those in Type I or Type III? Would privacy advocates prefer the robust tools in Type II or IV?

Third, the discussion will view the matrix no longer as a static chart but as a playing surface with moving parts. We will look at the dynamics of the chart, examining what happens, for example, when laws are introduced that attempt to push technologies from row to row or column to column. This will help us critique various classes of reform.

Up until now, we have treated the matrix like an Audubon guide for classifying privacy technology in the wild. Now, we will think of it more like the plans for a garden or farm, imagining the world of technology we want to inhabit, and judging and formulating policies to carry us to that world.

A. Applying Struggle to the Matrix

The harms from too much privacy and transparency described in Part II are at their worst with Type IV and Type I technologies. For example, consider the effects of Type IV tools. Robust privacy-enhancing tools worry the police, but much more if they are easy-to-use or come installed with computers by default. If tools like Skype and BitTorrent become widely used, the anonymity they provide will inspire fears of undetectable crime. These fears alone could spur law enforcement to seek new search and seizure laws and may convince judges and legislators that they deserve them. More police money would be invested in supporting the underground economy of spyware and virus writing. More indiscriminate monitoring would occur.

Similarly, a world of many Type I technologies would spur individual and collective harm and would make it difficult to dissent.[180] Of course, the same could be said of Type III tools, which also provide weak privacy. Privacy advocates likely worry more about Type I than Type III technologies, however, because Type I tools are more likely to deceive users. Users do not choose Type III tools because they expect privacy; instead, they choose Type III tools for the ease-of-use or affordability. Type I technologies, on the other hand, are costly; paying a Type I tool's costs might

[180] Usually, the market will take care of all of these fears by ensuring that Type I technologies do not arise or spread. But a world full of Type I technology could possibly be forced through laws and policies like CALEA and Clipper. Privacy advocates thus fear and oppose such laws with good reason. We will highlight forced Type I moves at the end of this Part.

create for the unsophisticated user the illusion of robust privacy. For example, people who pay the costs of setting up WEP wireless security may expect that, in return for their investment, they should receive privacy and security. These users, laboring under less privacy than they think they have, may act carelessly, sharing more information than they would if they had understood the circumstances.

This brief discussion is meant to illuminate the value of the matrix model and the struggle-enhancing ideals underpinning it. The matrix focuses attention on the crucial and easy-to-neglect cost dimension. When focusing on cost as well as robustness, analysts will start to ask nuanced questions which are unlikely to elicit entrenched, knee-jerk responses. For example, attention to the cost dimension would force advocates to think past simple questions (with obvious answers) about whether "robust or not robust" privacy-enhancing tools are better; instead, they would focus on more sophisticated, second-order considerations such as: what is the effect on dissidents if they have access only to "robust and high cost" tools without access to "robust and low cost" tools?

The matrix also makes it easier to focus on more than one tool at a time, discouraging analysts from focusing too narrowly on one technology. Just the spatial, visual image of the two-dimensional matrix itself reminds observers that there is an entire landscape dotted with tools that impact privacy and transparency. Participants who adopt this type of landscape view—instead of a narrower, one-tool-at-a-time view—can better weigh benefits and costs collectively. It may not matter if *this* Type III tool is insufficiently robust, the matrix model may lead us to conclude, because it is balanced by so many robust Type II tools. In contrast, when analysts focus on the spectrum, it is easier for them to obsess about *one* tool, imagining slippery slopes, turning the debate over a single technology into the battlefield where the war is won or lost.

The matrix and the struggle-enhancing view lead directly to compromise. The matrix helps participants understand the great variety of choices which may provide more room for leeway and negotiation. Unlike the spectrum, where every battle is zero-sum, with the matrix, losses along one axis may be offset by gains (or at least held ground) in the other dimension. Thus, the FBI agent can console himself by recognizing that although some developer has introduced a new, robust technology, it is hard to use; likewise, the EFF attorney can take solace in the fact that

the not-terribly-robust tool at least comes bundled with every version of Windows.

B. Good Enough Privacy—Hard but Possible

1. Hard but possible.

If Type I and IV technologies would raise the most significant and important risks of harm, then they should be avoided. If we could avoid these, we would find ourselves in a world of Type II and Type III tools. I call this a "hard but possible" world, and I will argue that it best avoids the harms discussed in Part II. It is the world of technology we should strive to create.

How are privacy and transparency allocated to different people in a world with only Type II and III technologies? First, because of the existence of Type II tools, those with sufficient resources who desire privacy can have it.[181] Everybody else would have to resign themselves to Type III tools, either because they would not care as much about privacy or because they could not afford privacy's costs.

Meanwhile, the police would find this world to be, perhaps reassuringly, much like today's world. Some criminals (and dissidents) would be very difficult to monitor, because of their use of robust tools. But because these robust tools, by definition, would be limited to those with resources, many people, perhaps the majority, would use Type III instead. Because Type III tools can be easily pierced, the police would enjoy a steady stream of successful investigations.

I call this mix of privacy and transparency, "hard but possible," because actors can get what they want, but only with hard work. Speakers who want to speak privately—criminals, dissi-

---

[181] Because fewer people will use encryption in a "hard but possible" world, those who use encryption may find themselves the target of increased government attention. Using techniques known as traffic-analysis, those conducting surveillance can tell that a particular user is using encryption, even if they cannot decipher the communications. See Richard A. Posner, *Privacy Surveillance, and Law*, 75 U Chi L Rev 245, 253 (2008) ("Traffic analysis is examining message length, frequency, and time of communication and other noncontent information that may reveal suspicious patterns; thus traffic analysis cannot be foiled by encryption because the information is not content based."); David A. Walker, *Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action*, 1999 Stan Tech L Rev 3, 23 ("In a world where encryption is the exception rather than the rule, it is much easier to determine who has something to hide as the encrypted, and presumably most interesting or highest value, messages stand out. If the time comes when most message traffic is encrypted, it will be impossible to determine which are the most secret messages in real time and the sheer volume of encrypted message traffic will make traffic analysis difficult.").

dents, and the merely paranoid—should be able to, provided they have the resources. The police would find it very difficult to catch the most resourceful, sophisticated speakers online, but as the earlier discussion of the Timberline High case demonstrates, even those speakers would be detectable with an investment of time, tools, and manpower.

2. How hard but possible reduces harm.

The hard but possible world's distribution of power and tools represents the best formula for minimizing privacy's and transparency's harms. So long as some suspected criminals use Type III tools—which should be plentiful given the lack of low-cost Type IV alternatives—the police would be able to track them. These successes, in turn, would give the police and their champions confidence in their continued ability to fight crime despite the spread of digital communication. Because of this confidence, they would be less likely to pursue legislative fixes, gray hat surveillance, and indiscriminate monitoring.

Not only would more arrests and convictions quell desires for new legal authorities, but when new laws *would* be sought, they would be less likely to be embraced by sympathetic legislators and judges because advocates on the other side would be able to point to the surveillance the police can still perform.

Likewise, the harms of perfect transparency would also be reduced because Type II tools would be available in the hard but possible world. People who manage to find, install, and properly use these technologies would enjoy robust privacy and everything it provides. They would be able to develop themselves through self-realization and would find a sense of repose. They would enjoy increased dignity and autonomy. All of society may benefit, as people would use Type II-bestowed privacy to fuel the debate over hard choices. Most specifically, if freedom fighters used Type II tools, they would be able to organize and agitate.

This is a very rosy picture of the hard but possible world. Unfortunately, the discussion masks one potentially ugly result of the world described. This result is clear when one examines *who* would get the benefits of privacy in this world.

3. Distributional concerns.

The crucial difference between a world full of Type II technologies and one with Type IV technologies is the fate of the unsophisticated criminal (or dissident).[182] In either world, extremely savvy (or wealthy) criminals would find technological privacy. But in the Type IV-rich world, the unsophisticated criminal would be able to hide while in the Type II-dominated world he would not.[183]

This disparity stems from a feature of Type IV tools: they protect users from surveillance, whether or not they ask to be protected. Every Skype user benefits from encryption, even if he does not care if his conversations could potentially be monitored. Every BitLocker user and almost every BitTorrent user will similarly receive more protection than he asks for or realizes he enjoys.

But if we did not have Type IV tools, if we lived in a hard-but-possible world, it would be the unsophisticated, the poor, and the powerless who suffer. They would be the bone thrown to the police to tamp down desires to engage in gray hat surveillance and enact new laws. In other words, "hard but possible" may be seen as the desire to give privacy only to the powerful and wealthy.

I worry about the distributional problem, but ultimately I resist the critique for many reasons. First, the "costs" in the matrix are not tied exclusively to traditional resources such as money or labor. The most important resource needed is technological know-how. A good hacker can download and install TOR with relative ease and for free. Furthermore, in a world where Moore's law is driving down the cost of computers; with Internet access more widespread than ever; and with an entire universe of

---

[182] Regulating the unsophisticated may have been the motive underlying the Clipper Chip. Although sophisticated users might have avoided the technology, the unsophisticated would not. As Steven Levy speculated at the time:

> The Government understands the impossibility of eradicating strong crypto. Its objective is instead to prevent unbreakable encryption from becoming routine. If that happens, even the stupidest criminal would be liberated from the threat of surveillance. But by making Clipper the standard, the Government is betting that only a tiny percentage of users would use other encryption or try to defeat the Clipper.

Steven Levy, *Battle of the Clipper Chip*, NY Times 6 (June 12, 1994).

[183] See Froomkin, 143 U Pa L Rev at 796–97 (cited in note 5) ("Clipper's critics suggest that it can catch only stupid criminals. . . . The least subtle response has been that criminals are often dumber than one thinks.").

free, and freely available, open source operating systems and tools, the opportunity to master computers would be available very far down the socioeconomic stratum. Contrast this with molecules-not-bits technologies, which often require expensive tools to master.

Of course, this argument should not be overstated. There are many, many hurdles that prevent a poor person from becoming a hacker. Although computers and Internet access are cheaper than they have been before, they are still expensive to many. Also, technological mastery requires not only tools but free time, something that the poor have in short supply. In fact, wealthy people have an advantage that even the moderately wealthy may not: without ever mastering the technology, they can simply *buy* technological privacy; they would not need to become hackers, because they could pay other hackers to protect them.

A second response is that while the possibility of distributional inequality should raise concerns, these concerns likely do not offset the harms described in Part II. The harms from too much privacy—of gray hat surveillance, draconian new laws, and unsolved crime—are profound, and they need to be addressed, perhaps even if the solution means privacy is handed out according to preexisting inequalities. This is especially true if some of the harms from too much transparency—especially indiscriminate surveillance and broad new surveillance laws—could be used disproportionately to disadvantage the same disadvantaged groups.

This is another way of saying that there are many, many distributional concerns in our society, and that identifying one more should raise serious concerns but cannot serve by itself to indict.

Third, there may be ways to soften distributional inequalities. For example, consider the freedom fighter again. Freedom fighters, who are often poor, should be empowered by sympathetic, wealthy individuals, organizations, and governments who support their causes. People should find ways to supply money, technological know-how, training, computer hardware, and software tools directly to oppressed freedom fighters. Consider, for example, the work of Dr. Patrick Ball, Deputy Director of the Science and Human Rights Program with the Association for the Advancement of Science. Through AAAS, Dr. Ball has worked extensively with "grassroots non-government human rights or-

ganizations and truth commissions to build information management systems."[184] Much of this work involved helping groups use tools of privacy and anonymity.[185] In many cases, governments should share this burden. Imagine the Voice of America/Radio Free Europe, but with code. Rather than making privacy-enhancing software simply easier to use, with the end result of moving tools from Type II to Type IV, resources could instead be used to help chosen individuals struggle against totalitarians.

C. Enforcing Struggle

Finally, having established the value of hard but possible, good enough privacy, let us conclude this Article by looking at prescriptions that push the world in this direction. According to Professor Lawrence Lessig, four forces regulate online behavior: markets, norms, code, and law.[186] These forces have each played a role in the evolution of privacy and transparency, albeit often through unintentional decisions and without a systematic vision of technological privacy and technology.

How can these four online regulators be used to push the world away from Type I and Type IV and into Type II and Type III tools? Consider them in turn.

1. Markets.

Markets already seem to select against Type I and IV technologies. Both types are rarely seen and hard to come by. The examples presented in this Article—WEP (Type I), Skype, BitTorrent, and BitLocker/EFS (all Type IV)—are exceptions.

Perhaps markets do not produce many Type IV tools because people undervalue information privacy. This is an empirical, not normative, claim. Especially because measures to secure privacy are expensive, and because the harms from invasions of privacy are often diffuse, market forces do not push software developers to invest heavily in protecting privacy.

BitLocker/EFS, Skype, and BitTorrent are exceptions. These are all recent examples, and perhaps they mark a shift in the market, reflecting more consumer price sensitivity to privacy.

---

[184] Affidavit of Patrick Ball, *ACLU v Miller*, available at <http://www.aclu.org/privacy/speech/15525lgl20031009.html> (last visited Apr 4, 2008).

[185] Id.

[186] Lawrence Lessig, *Code Version 2.0* 123–25 (Basic 2006).

BitLocker/EFS, in particular, seems to support this theory. In 2002, Microsoft very publicly shifted resources and attention to improving the security of its code.[187] Microsoft's executives concluded that the constant barrage of vulnerabilities in the Windows Operating System, in particular, was beginning to wear on customers who were increasingly aware of identity theft.[188] For example, it was widely reported around that time that as many as five thousand employees were pulled off assignments for months to attend security refresher courses.[189]

But it is difficult to tell whether Microsoft's newfound sensitivity to privacy and security represents a shift in the market or whether it instead is specific to this company. In fact, there is even some doubt whether Microsoft will continue to invest so heavily in security. The company may be chastened by the many reviewers who have complained about the overbearing security measures in Windows Vista.[190]

In contrast to the story at Microsoft, Skype and BitTorrent more likely reflect outliers, products of other pressures and not part of a trend to more Type IV encryption. Some BitTorrent programmers added encryption to protect a particular kind of privacy—privacy against ISPs.[191] ISPs have begun slowing down the speed of their networks for users who have been trading many large files using BitTorrent.[192] Developers changed versions of the BitTorrent client in response, converting them from

---

[187] Kevin Maney, *Microsoft Shifts Its Focus to Security*, USA Today 1B (Jan 17, 2002) (reporting memo from Bill Gates to Microsoft focus announcing a shift of priorities to focus more on security).

[188] Id.

[189] Peter Judge, *MS Spends $100M on Security Tutorials*, ZDNet News.com (July 2, 2002), available at <http://news.zdnet.com/2100-3513_22-941159.html> (last visited Apr 4, 2008).

[190] Mike Masnick, *Did Microsoft Focus Too Much on Security in Vista?*, Techdirt Blog (Nov 29, 2007), available at <http://www.techdirt.com/articles/20071127/022730.shtml> (last visited Apr 4, 2008) ("It turns out that, while security *is* important to users, it's not so important that it comes at the expense of other things—like stability and compatibility. In other words, while focusing on security, Microsoft may have dropped the ball on other features that actually are more important in the buying and upgrading decisions.") (emphasis in original).

[191] Ernesto, *How to Encrypt BitTorrent Traffic*, TorrentFreak Blog (Apr 16, 2006), available at <http://torrentfreak.com/how-to-encrypt-bittorrent-traffic/> (last visited Apr 4, 2008) (noting that encryption was being added to BitTorrent clients to take out ISP "traffic shapers").

[192] Peter Svensson, *Comcast Blocks Some Internet Traffic*, AP (Aug 19, 2007), available at <http://rss.msnbc.msn.com/id/21376597/> (last visited Jan 30, 2008) ("Comcast Corp. actively interferes with attempts by some of its high-speed Internet subscribers to share files online.").

Type III to Type IV tools to protect a narrow type of privacy against a narrow type of monitoring.

Skype's path to Type IV status is no less idiosyncratic. Skype is a peer-to-peer service. Phone calls are sent efficiently over the Internet by enlisting other Skype "peers"—other computers running Skype—to help carry the traffic along. Early on, it was understood that malicious peers might be able to listen in to third-party phone calls. Thus, encryption was seen as necessary to convince users to trust the network.[193]

Although all three of these stories are examples of developers improving the privacy of their programs, they do not seem to suggest a great awakening on the part of consumers to information privacy concerns they have neglected for years. Instead, they seem like three special cases that do not necessarily signify a trend.

2. Norms.

Legal scholars have not discussed the norms of technological secrecy and privacy. We know that most people tend not to bother using encryption at all, aside from the built-in, Type II, encryption that comes bundled with our web browser.[194]

There is some interesting and useful work in computer science that deserves to be imported. For example, researchers at Princeton led by Shirley Gaw interviewed the activist-employees of a "non-violent direct action organization."[195] In the words of the study's authors, these employees "had opponents working against them, they had secrets to protect, and colleagues' freedom was at stake when security failed."[196] In short, these were people one would expect would use encryption.

What the researchers learned instead was that only a few of their interviewees used encryption, and even those people limited their use to certain situations. In particular, employees who

---

[193] Templeton, *Is Strong Crypto Worse* (cited in note 20) ("Skype's architecture routinely routes voice traffic through other Skype users with real IP addresses in order to get past NATs. Had they not encrypted, nasty users running these supernodes would be routinely listening in on the calls going through them.").

[194] See Freier, Karlton and Kocher, *The SSL Protocol* (cited in note 73) (describing SSL).

[195] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly, *Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail*, Proceedings of CHI 2006 Conference on Human Factors in Computing Systems 1 (April 22–27, 2006), available at <http://www.cs.princeton.edu/~sgaw/publications/01Feb-Activists-sgaw-CHI2006.pdf> (last visited Apr 4, 2008).

[196] Id.

handled the logistics of the group's "actions"—defined as "the high-profile events staged by activists"[197]–and who tracked donors and donations encrypted email messages.[198] Even those employees limited the use of encryption to secret information.[199]

How does this research answer the question presented in this Part—can norms be used to push away from Type I and IV technologies? To answer this, we first need to do some translation to offset an implicit bias in the work. These researchers—like most computer scientists who research encryption—start from the assumption that encrypted email deserves to be "universal and routine."[200] Perhaps because of this starting point, their conclusions and prescriptions tended to revolve around how tools could be made more usable to make encryption more common.[201] In other words, they concluded that the norms have failed to push software to Type IV—where they "deserved" to be—and recommended efforts to bring about more Type IV tools as a remedy.

But when one steps back from this bias, one can see that norms more directly regulate behavior in a world of Type II and III technologies than in a world of Type IV technologies. For example, many employees seemed to see the use of encryption as a signal or flag of the secrecy of a message. One employee expressed his annoyance, for example, at a co-worker who encrypted mundane messages.[202] This signaling feature would be lost if the organization switched to a Type IV, effortless encryption method.

Other employees elaborated on this role of encryption as a "flagging" mechanism. An employee discussed how there were norms of politeness bound up in encryption: if a message was sent encrypted, it was expected that replies would also be encrypted.

Finally, several employees saw the use of technological privacy as paranoid and not for "normal people."[203] It was also seen

---

[197] Id at 3 n 2.

[198] Id at 6.

[199] Gaw, Felten, and Fernandez-Kelly, *Secrecy, Flagging, and Paranoia* at 4 (cited in note 195) (discussing employees with pseudonyms Woodward and Abe).

[200] Id at 1.

[201] Id at 8–9.

[202] Id at 7 (quoting "Abe," "I get this message and—oooh, it's encrypted. 'Can we have a meeting tomorrow at 2:00?' I'm like, what's the secret?").

[203] Gaw, Felten, and Ferndandez-Kelly, *Secrecy, Flagging, and Paranoia* at 7 (cited in note 195).

as something for techies, something with a high "gadget factor."[204] In sum, norms have pushed the use of encryption in this organization into a hard but possible mix. Encryption is hard to use but robust, and norms of politeness and respect for hierarchy cause important messages—those involving the group's actions and donors—to be encrypted, while the rest are not.

One concern with incorporating this research into the matrix is the confounded causes and effects. Many of the conclusions of the paper *stem from* the fact that the encryption tool used by the organization was difficult to use.[205] If the organization instead had access to Type IV technology, perhaps the norms would have been very different. Technology shapes norms just as much as norms dictate technology. Because of this complex relationship, there are limits to what can be concluded from these observations about norms and the technology of privacy and transparency. More work should be done in determining how this Article's prescriptions relate to past, present, and evolving norms.

3. Code.

Most of all, it is hoped that software developers appreciate better the complex and potentially fraught world of too much privacy. When these developers see privacy as an irreproachable good, their conscious and unconscious choices will lead to more robustness and easier-to-use solutions. This may push their tools into Type IV.

Computer scientists, for example, talk about the "grand challenge" of providing secure email.[206] Although these researchers are focused, in large part, on the complexity of getting the various forms of encryption to work,[207] it is evident that much of the challenge comes from making secure email easy to use.[208] Researchers engaged in the grand challenge never seem to stop to discuss whether easy-to-use secure email is desirable.[209] The con-

---

[204] Id at 4 (quoting Abe).

[205] Id at 8 ("Critics may argue that ActivistCorp had adopted the least usable form of the technology. Had employees adopted implementations like HushMail, CryptoHeaven, or S/MIME support in e-mail clients like Thunderbird or Outlook, perhaps they would have encrypted more frequently or with fewer complaints.").

[206] Garfinkel, *Thesis: Design Principles and Patterns* at 161 (cited in note 156).

[207] Id (describing the difficulty of the challenge as being that it "requires that many other problems be solved first.").

[208] Id at 168 (critiquing the "usability" of a commonly used secure email protocol called S/MIME).

[209] Shirley Gaw, for example, in the first line of her interesting paper on the norms of

clusion is assumed, and it would probably seem ridiculous to them to suggest otherwise.

Developers implementing encryption should consider whether "ease of use" is always the best option. For example, consider software defaults. Studies show that privacy-enhancing software that is shipped "turned off" by default is very likely to remain off. As a result, software defaults can make an otherwise Type IV technology act like a Type III tool instead. For this reason, Microsoft's decisions to disable BitLocker by default and to keep BitLocker and EFS out of "home" versions of their Vista operating system are significant. [210]

This advice applies not only to developers. Privacy advocates investing in privacy-enhancing technologies should consider investing more in projects that improve tool robustness and less in projects designed to make software easier to use. Groups motivated by the concern that dissidents need encryption to speak freely should consider investing in training dissidents, rather than making a tool so easy to use that anybody—dissident, criminal, and ordinary user alike—will be able to take advantage.

4. Law.

Almost every past attempt by the U.S. government to regulate encryption has suffered from the same fatal flaw: each time it has tried to force tools to be Type I. For all of the reasons described in this Article, it is a disaster to force Type I tools on people by regulation. Type I tools raise starkly the harms of too much transparency. Privacy advocates and computer scientists understand this, which explains their fierce opposition to past proposals.

Clipper tried to push onto an unwilling market an encryption scheme that was completely transparent to government officials holding escrowed keys.[211] CALEA forces providers to engineer systems to allow quick, easy access to communications by government agents.

---

encrypted e-mail starts with the question, "What will it take to make the use of encrypted e-mail universal and routine?" Gaw, Felten, and Fernandez-Kelly, *Secrecy, Flagging, and Paranoia* at 1 (cited in note 195). She never pauses to ask the question, "Is universal and routine encrypted e-mail desirable?"

[210] Morris, *Notes on Vista Forensics* (cited in note 76).

[211] See Froomkin, 143 U Pa L Rev at 741 (cited in note 5) ("[B]reaking through Clipper's protections will involve no (computational) effort for authorized persons because the government will keep a copy of the keys.").

In both cases, the government has repeatedly argued that the opposition's concerns about too much transparency were overblown not because they were untrue, but because the government promised to use organizational and bureaucratic controls to replace the dissolved technological barriers. Thus, Clipper's escrowed keys would be split in two pieces and handed to different executive branch agencies.[212] Likewise, CALEA gives the police no affirmative authority to monitor, it just smoothes the way for an agent with a warrant or court order to access communications quickly.

These responses are not untrue. With CALEA and Clipper, the government *did* impose bureaucratic and legal controls. But these types of controls can be repealed or modified,[213] and for that reason, they are almost besides the point in the discussion over technological privacy and transparency. This is why organizational and bureaucratic constraints do not appear in the matrix model presented above. These types of constraints are valuable, and should be debated and scrutinized, but they are a non sequitur when it comes to measuring the potential harms described in Part II.

A better CALEA would have been one that tried to engineer struggle instead of perfect transparency. Perhaps CALEA could have been written to limit the key length on provider supplied encryption, allowing the police the chance to crack communications through brute force computational methods, but only at great cost; this would have made decryption hard but possible. Or perhaps CALEA could have targeted the spread and ease of use of privacy-enhancing technology, rather than the robustness. It could have, for example, prevented providers from supplying privacy-enhancing tools like encryption to users by default. Users could opt-in to encryption, but the ordinary user probably would not.

There is an important, more general point. The government has repeatedly tried, and will no doubt in the future try again, to impose vulnerabilities in encryption. Each time it has done this, it has tried to swing for the fences—to force people to move all the way from perfect privacy to perfect transparency. Next time,

---

[212] The designated agencies were the Department of Commerce's NIST and the Treasury Department's Automated Systems Division. Id at 759 & n 204 (citing US Department of Justice, Press Release, *Attorney General Makes Key Escrow Encryption Announcements* (Feb 4, 1994), available at <http://www.cpsr.org/prevsite/program/clipper/reno-key-escrow-announcement.html> (last visited Apr 4, 2008).

[213] See Froomkin, 143 U Pa L Rev at 782–86 (cited in note 5).

perhaps it should try to hit a single instead, trying to mandate weaker, but not weak, encryption. These more modest goals do less to bring about the harms described in Part II.

But how would the government weaken without crippling encryption? One obvious way would be to regulate key length, but there would be limits to this approach. With most cryptographic systems, brute force decryption can be sped up by using computers in parallel.[214] Roughly speaking, four computers can decrypt four times more quickly than one computer. Thus, what may seem impenetrable to the typical observer may turn out to be surmountable for the government agency with ample resources.

But there are better alternatives to regulating key length, found in some interesting cryptographic research. In a sense, these implement hard-but-possible through technology. For example, Ron Rivest, the noted cryptographer who co-invented the RSA public key cryptography system has discussed what he calls timed-release cryptography.[215] These are encryption methods that can be broken through brute force methods, but that are guaranteed to require a set period of time to crack. In other words, these are methods designed to thwart the use of parallel computers. Without getting into all of the details, these methods are designed to force would-be decrypters to attack the problem one step at a time, which would prevent them from using more computers to solve the problem in less time. In Ronald Rivest's words, these techniques are "intrinsically sequential."[216]

---

[214] Ronald L. Rivest, Adi Shamir, and David A. Wagner, *Time-Lock Puzzles and Timed-Release Crypto* (1996) available at <http://citeseer.ist.psu.edu/87499.html> (last visited Apr 4, 2008).

[215] Aldar C-F. Chan and Ian F. Blake, Scalable, *Server-Passive, User-Anonymous Timed Release Cryptography*, Proceedings of the 25th IEEE International Conference on Distributed Computing Systems 504–13 (2005); Rivest, Shamir, and Wagner, *Time-Lock Puzzles* (cited in note 214).

[216] Ronald L. Rivest, *Description of the LCS35 Time Capsule Crypto-Puzzle* (Apr 4, 1999), available at <http://people.csail.mit.edu/rivest/lcs35-puzzle-description.txt> (last visited Apr 4, 2008). In 1999, in honor of the 35th anniversary of MIT's Laboratory for Computing Science, Ronald Rivest encrypted a message using a timed-release crypto method and presented the ciphertext to Frank Gehry, who was designing LCS's new building. At the time, Professor Rivest explained, "We estimate that the puzzle will require 35 years of continuous computation to solve, with the computer being replaced every year by the next fastest model available. Most of the work will really be done in the last few years, however." Id.

Another possibility is known as translucent cryptography.[217] Building on some earlier work by others, in the middle of the Clipper debate, Rivest again (writing with others) proposed an encryption scheme that would yield to keys held by the government, but only some of the time, creating probabilistic surveillance. For example, if the "p" value of the translucent cryptography was tuned to a value of 0.02, the police with access to ciphertext and the proper key would be able to crack the encryption in 2 percent of the cases.

This is "hard but possible" in action. If a CALEA-like law or a Clipper-like quid pro quo scheme tried to force users to use timed-release or translucent cryptography instead of force perfect transparency, it would shift the balance between speakers and surveillers, but without shifting all the way to perfection. Not only would this approach ameliorate the harms of too much transparency, it would perhaps encounter less fierce opposition. Both of these solutions arose even though the market tended to discourage hard-but-possible thinking in cryptography. Imagine the even more revolutionary proposals that might arise if the NSF decides to fund such a project.

I do not want to be overly sanguine about the public's likely embrace of compelled use of any of these techniques. The average cypherpunk will see little difference between Clipper's and CALEA's perfect transparency and these hard but possible techniques. In fact, it is the compulsion—the inability to choose—that offends. Yet I do hold out hope that such critics would instead see hard but possible as a more moderate position, one that would preserve—through code—a level playing field. Even if these particular schemes were insufficiently "hard," perhaps there would be others, extant or that would be invented, that would satisfy.

CONCLUSION

This Article has tried to bridge a divide which causes pro-privacy and pro-transparency advocates to shout past one another. On the pro-privacy side, I am including a fairly well-defined group: privacy advocates at EFF, the Electronic Privacy Information Center, and the Center for Democracy and Technol-

---

[217] Consider Mihir Bellare and Ronald Rivest, *Translucent Cryptography: An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transfer*, 12 J Cryptology (Oct 1999).

ogy; and the legal scholars who have been recently twice-branded as the "New Privacy" scholars[218] and as members of the "Information Privacy Law Project."[219] These participants view information privacy as a fundamental right, and in fact place information privacy on a privileged deontological plane, focusing not only on traditional conceptions of individual rights, but recasting the interest as societal, focusing on privacy's role in securing individual autonomy, dignity, and deliberative democracy that flow from the exploitation of personal information.

Opposed to these participants is an eclectic group of people, more different than alike but tied together by a focus on traditional utilitarian balancing tests and market-based conceptions of privacy. These participants range from law enforcement officials, to privacy-as-property market-driven libertarians, to Internet-Fourth Amendment scholars, to communitarians, to national security hawks.

These two sides are not engaging one another, but this does not seem to be a matter of benign neglect; the two sides seem simply unconvinced by one another's arguments. Granted, each side will often pay lip service to the other, being careful always to extol the virtues of the values described by the other side. "Privacy is indeed important," says the scholar about to urge for less of it. "The need to protect our security is unquestionable," responds her colleague, just before questioning it. One suspects, however, that neither side truly believes the other side's claims. There is an air of cordiality that needs to be stripped away, making the choices more starkly presented.

This polite, disengaged rhetoric troubles those of us who believe the claims made by both sides. Security is an important goal, and given the fear—rational or not—we feel about terrorism, we hope the government can think of new ways to defend us from future attacks, and we are probably willing to give up some privacy for greater security. But we also credit the New Privacy scholar's descriptive and normative claims about privacy, valuing our privacy deeply and believing claims about the importance of privacy for self-determination, autonomy, and deliberative democracy. Furthermore, we are chastened by the lessons of history: balancing away such interests in the face of some security

---

[218] Paul M. Schwartz and William M. Treanor, *The New Privacy*, 101 Mich L Rev 2163, 2177 n 33 and accompanying text (2003).

[219] Neil M. Richards, *The Information Privacy Law Project*, 94 Geo L J 1087, 1089 n 6 (2006).

threat has proven too easy to do, and one wonders whether we can change the terms of the debate to better respect the values of privacy.

The problem with balancing two equally important and seemingly unmoving interests is that anytime one side prevails on any narrow set of facts, the other side—engaged as it were in a game of brinksmanship—views the result as a loss. This is the "Thunderdome" approach to balancing, a zero-sum endeavor where two opposing principles enter, and only one can emerge victorious.

The solution—or better yet, one solution—is struggle. Although it is a small change, a tweak, on one's perspective, it may pay great dividends. By redefining the debate about something other than balance, by defining a new normative value—hard but possible communication and investigation, and by identifying a mechanism—struggle—for realizing that value, this Article has offered an alternative vocabulary for discussing the virtues of both privacy and transparency.